Expanding the Boundaries of Internal Controls

MODERATOR  Deb Muller
Chief Financial Officer, Volusia County School District

SPEAKERS  Roland Svensson
Senior Consultant, Swedish Association of Local Government Finance

Jorg Bassek
Chief Administrative Officer, Borlänge municipality

Jeff Wright
Senior Manager, Plante Moran
Expanding the Boundaries of Internal Control
GFOA - Denver
2017-05-22
Should we take the risk......?
Don’t be scared to try something new – the grass might be greener on the other side!
Thank you for listening!

Roland Svenssson, KEF Sweden
Management control model
Quality management system
Supposition

- Processes run across several different operations/businesses

- Steps of the process are the same regardless of operation/business

- Purpose and use/application determines which legislation governs the errand and which business-specific management system that enter

- Risk management should be done in a similar way in all operations/businesses
Control chart for stability analysis
How to do it

Plan
Identify and analyze risks

Decisions as controls

Do
Control activities throughout the organization

Check
Decision on corrective actions

Act
Corrective actions

Quality assurance system

Reports
Success factors

- Incorporate and simplify
- Management's commitment
- Provide guidance and support to those involved in the process
Each management team identifies and analyzes risks.
The city council has the overall responsibility that controls and risk mitigation measures are kept at an acceptable risk level.
<table>
<thead>
<tr>
<th>Område</th>
<th>Risknivå</th>
<th>Åtgärd</th>
<th>Resultat</th>
<th>Effekt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports of external companies’ costs for clients within LSS do not match actual costs.</td>
<td>18</td>
<td>A review and examination of all reports.</td>
<td>A deviation of 919 280 SEK</td>
<td>A new reporting system in place. Quality assurance procedures developed.</td>
</tr>
<tr>
<td>Prior assessments for children/adolescents up to 18 years according to the law of SoL.</td>
<td>17</td>
<td>A review of completed prior assessments during a limited period of time (2 months).</td>
<td>Deviations from regulations were found</td>
<td>Routines and procedures developed and anchored for the reception team, postal management and documentation.</td>
</tr>
<tr>
<td>The rehabilitation process</td>
<td>17</td>
<td>A review to make sure managers follow set routines.</td>
<td>The review showed that in 80% of the cases, manager had deviated from the routine</td>
<td>The rehabilitation process has been revised and educational efforts have been implemented.</td>
</tr>
<tr>
<td>Organized fraud of granted benefit</td>
<td>17</td>
<td>A review to make sure managers follow set routines.</td>
<td>In 50 of 3306 apartments there were unauthorized second hand subleases.</td>
<td>A new external review of a specific area.</td>
</tr>
</tbody>
</table>
Our review showed that in 80% of the cases, manager had deviated from the routine to contact the sick employee at the 80:th day.
Protect Value by Managing Risk

ENTERPRISE RISK MANAGEMENT (ERM)

Government Finance Officers Association | May 22, 2017
Introduction

JEFF WRIGHT, CPA, CIA, PMP
Senior Manager, Enterprise Risk Services
312.602.3530
Jeff.Wright@plantemoran.com

Jeff is a Senior Manager in the Plante Moran – Management Consulting division. He is one of the Chicago leaders of the Enterprise Risk Services group which helps clients with risk management, internal audit and regulatory compliance.
What is Enterprise Risk Management (ERM)?

The Committee of Sponsoring Organization (COSO) defined ERM in 2004 (2016 Update Comment Period closed 12/15/16):

Enterprise risk management is a process, affected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and Manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.
“What do these government organizations have in common?”

**Harvey, IL:** Issues bonds to develop a hotel in town but uses funds to cover payroll.

**Penn State University:** Board of Directors cover up of child abuse scandal.

**State of New Jersey:** Governor subject to investigation of bridge closure scandal.

**Ramapo, NY:** Town officials allegedly fabricated financial statements to fraudulently raise money in the bond market to pay for a new minor-league-baseball stadium.

**New York City:** Science Applications International Corp (SAIC) defrauds the City more than $500M in overpayments on the CityTime payroll IT project.

**Dixon, IL:** Fraud risk from Treasurer caught embezzling $54M over 2 decades.

**U.S. Govt. Office of Personnel Management:** Data of 18 million employees hacked.

**State of Alabama:** Governor resigns to avoid impeachment after alleged affair.
An organization must ensure that the risk management environment occurs on an enterprise-wide approach vs. a silo approach. Monitoring controls are established at the entity level for a company-wide view of risk taking to account for risk objectives from each process.
Evolution of Risk Management

- **1960s**: Insurable Risk
  - Risks based on historical loss experience and for which insurance policies can be purchased:
    - Property/Casualty
    - Errors & omissions
    - Liability
    - Workman’s compensation
    - Fire/Flood

- **1970s**: Quantifiable Risk
  - Financial instruments emerged and shifted focus to quantitative risk and other management tools:
    - Earnings at risk
    - Value at risk
    - Historical predictors
    - Monte Carlo simulations

- **1980s**: Enterprise Risk
  - Risks are classified as:
    - Strategic
    - Finance/Reporting
    - Operational
    - Compliance
  - Management uses a top-down approach to identify, measure, and mitigate risks

**Today’s Focus**

- **2000s**
- **2010s**
Two Most Common Myths About ERM

MYTH #1:
ERM is a process only handled by the chief financial officer or finance.

FACT #1:
The ERM risk universe consists of strategic, financial, operational and compliance risks. All members of senior management are needed to participate in the ERM process to have adequate knowledge and experience with the various risk strategies required. ERM does not lie within finance alone.
Two Most Common Myths About ERM

**MYTH #2:**
ERM is a periodic event that requires updates only quarterly, semi-annually or annually.

**FACT #2:**
ERM is a process just like any other process within the organization (payroll, inventory, revenue, accounts payable, etc.). The ERM process for each company are at different stages of maturity. Keep in mind that ERM is a JOURNEY, not a destination. Your risk profile is continuously changing and your ERM process to adapt with your risk profile.
ERM Development Overview

**INPUTS**

**STEP 1**
Assess Internal Environment, Understand Objective Setting and Risk Profile, Build Out Risk Universe and Infrastructure Pyramid

**STEP 2**
Perform participant Polling to determine Impact & Likelihood Analysis for Inherent Risk

**STEP 3**
Hold Risk Workshop to risk rate Mitigating Activities and calculate Residual Risk

**STEP 4**
Develop Risk Treatment, Strategies and potential improvements to Control Activities

**STEP 5**
Deliver Risk Model with rankings and Key Risk Indicators (KRI’s) and Monitoring Controls for ERM Committee

**OUTPUTS**

- Risk register with customized risk universe
- Risk summaries with detail treatment strategies and risk playbook
- Robust ERM infrastructure with reporting and monitoring controls
Step 1: ERM Infrastructure Pyramid

ERM INFRASTRUCTURE

City Council
Mayor
ERM Committee

RESPONSIBILITIES

Approve ERM Charter, Assign Authority, Board Oversight
Program sponsorship, establish tone at the top, delegate authority, report to Council
Program Coordination, establish Policy & Procedures, create monitoring controls, assign risk owners and reporting protocols

Risk Owners: Monitor risks and report back to ERM Committee
Control Owners: Perform risk monitoring of Key Risk Indicators (KRI’s) and report back to Risk Owners

INFORMATION FLOW

1st Line of Defense

Financial Risk Owners
Strategic Risk Owners
Operation Risk Owners
Compliance Risk Owners
Controller, Finance Mgr
Mayor, Sr. Mgmt, Legal
City Mgr, HR Mgr, Svc Mgrs
HR Mgr, Compliance Mgr, Safety Mgr
Sample – Government Risk Universe (40)

<table>
<thead>
<tr>
<th>Strategic (15)</th>
<th>Operating (15)</th>
<th>Financial (6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational Structure</td>
<td>Service Failure</td>
<td>Accounting / Reporting</td>
</tr>
<tr>
<td>Employee Misconduct</td>
<td>Access to Talent</td>
<td>Legal Risk</td>
</tr>
<tr>
<td>Legislative</td>
<td>IT Governance</td>
<td>Fraud</td>
</tr>
<tr>
<td>Economic Slowdown Risk</td>
<td>Health Epidemic</td>
<td>Treasury / Liquidity</td>
</tr>
<tr>
<td>Governance</td>
<td>Infrastructure</td>
<td>Litigation</td>
</tr>
<tr>
<td>Reputation</td>
<td>System-wide Network/utility Failure</td>
<td>Insurance Gap</td>
</tr>
<tr>
<td>Stakeholder Expectations</td>
<td>IT Infrastructure</td>
<td></td>
</tr>
<tr>
<td>Budget/ Financial Planning</td>
<td>Natural Disaster</td>
<td>Federal Programs</td>
</tr>
<tr>
<td>Funding Availability</td>
<td>IT Security</td>
<td>Contract Compliance Risk</td>
</tr>
<tr>
<td>Innovation</td>
<td>Physical Assets</td>
<td>Health &amp; Safety (OSHA)</td>
</tr>
<tr>
<td>Culture</td>
<td>Environmental</td>
<td>Data Privacy/ HIPAA</td>
</tr>
<tr>
<td>Transparency</td>
<td>Authority/ Limit Risk</td>
<td></td>
</tr>
<tr>
<td>Management Oversight</td>
<td>Employee Turnover</td>
<td></td>
</tr>
<tr>
<td>Illegal Acts</td>
<td>Terrorism</td>
<td></td>
</tr>
</tbody>
</table>

**Compliance (4)**
- Federal Programs
- Contract Compliance Risk
- Health & Safety (OSHA)
- Data Privacy/ HIPAA
Step 2: ERM – Objective Definitions

**Risk:** The possibility of an event occurring that may have either a positive or negative impact on the achievement of objectives

**Inherent Risk:** The impact and likelihood of a risk event occurring BEFORE consideration of mitigating controls or circumstances.

**Mitigating Activities:** The internal controls or safeguards in place to decrease the chance of a risk event from occurring.

**Residual Risk:** The impact and likelihood of a risk event occurring AFTER consideration of a risk event occurring.
# SAMPLE - Impact & Likelihood Criteria

## Impact Criteria – Inherent Risk

<table>
<thead>
<tr>
<th>Ranking</th>
<th>5 (high)</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1 (low)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial – increased expense or lost revenue or lost funding:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt;$1M</td>
<td>$750K - $1M</td>
<td>$500K - $750</td>
<td>$250K - $500K</td>
<td>&lt;$250K</td>
<td></td>
</tr>
<tr>
<td>or Strategic:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure of overall strategic plan</td>
<td>Failure to meet multiple strategic objectives</td>
<td>Failure to meet 2 or more strategic objectives</td>
<td>Failure to meet 1 strategic objective</td>
<td>Minimal impact on 1 strategic objective</td>
<td></td>
</tr>
<tr>
<td>or Operational:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process or system Shutdown</td>
<td>&gt;3 Days</td>
<td>24 – 72 hours</td>
<td>12 – 24 hours</td>
<td>4 – 12 hours</td>
<td>&lt; 4 hours</td>
</tr>
<tr>
<td>Service Delivery Quality</td>
<td>Inability to provide an essential service</td>
<td>Serious impact to overall quality of essential service</td>
<td>Moderate impact to overall quality of essential service</td>
<td>Limited impact to overall quality of essential service</td>
<td>Limited impact of secondary service</td>
</tr>
<tr>
<td>or Regulatory:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Federal Govt./ EPA/ OSHA/ HIPAA</td>
<td>Large-scale Material breach of regulation</td>
<td>Material breach but cannot be rectified</td>
<td>Material breach which can be readily rectified</td>
<td>Minimal breach which cannot be rectified</td>
<td>Minimal breach which can be readily rectified</td>
</tr>
</tbody>
</table>

## Likelihood Criteria – Inherent Risk

<table>
<thead>
<tr>
<th>Ranking</th>
<th>5 (high)</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1 (low)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability of an event occurring in a given year:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt;50%</td>
<td>20 – 50%</td>
<td>10 – 20%</td>
<td>5 – 10%</td>
<td>&lt;5%</td>
<td></td>
</tr>
<tr>
<td>or Event Occurrence (on average):</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Once a year or more</td>
<td>1 in 3 years</td>
<td>1 in 5 years</td>
<td>1 in 7 years</td>
<td>1 in 10 years</td>
<td></td>
</tr>
</tbody>
</table>
Step 3: Risk Workshop
Assess the Strength of Mitigation Activity

A scale of 1 to 3 is used to evaluate the quality of mitigating activities currently in place, as shown below:

**Impact:** How strong is the control environment?

1 = Weak: Vulnerable control environment, limited visibility, no monitoring controls, immature process, no management attention/ awareness

2 = Moderate: Some internal controls exist, management evaluates periodically, limited visibility/ process

3 = Strong: Robust control environment has continuous monitoring with mature risk mitigation strategies in place

**Likelihood:** How likely is the mitigation activity going to mitigate the risk?

( 1 = Not Likely,  2 = Likely,  3 = Very Likely)

Multiply the Impact X Likelihood to calculate the Mitigation Activity score
Net Residual Risk (NRR) Score

NRR Formula

Inherent Risk Score:  
\{\text{Impact} \times \text{Likelihood}\}

(\text{-}) Less:

Mitigation Activity Score:  
\{\text{Impact} \times \text{Likelihood}\}

= NRR Score

Example:

Cybersecurity Risk

Inherent Risk:
- Impact = 4
- Likelihood = 5
- Total = 20 (4\times5)

Less: Mitigation Activities:
- Strong = 3
- Likely = 2
- Total = 6

NRR = 14 (20 - 6)
Step 4: Risk Treatment Strategies

We assess mitigation activities for identified risks to assist in the development of risk treatment strategies and plans:

Treatment Strategies:
1. Avoid
2. Accept
3. Reduce
4. Transfer
Step 5: Risk Model and Monitoring Activities
ERM Solutions: Risk Dashboard

0-8 = Below Tolerance, 9-16 = Tolerable Range, 17-25 = Above Tolerance
X = increasing Velocity, | = Stable Velocity
Key Risk Indicators (KRI’s)

3 Types of Data Sources:

<table>
<thead>
<tr>
<th>Data Source</th>
<th>KRI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Public Available Information</td>
<td>Risk Owner Monitoring:</td>
</tr>
<tr>
<td>• Economic Slowdown Risk</td>
<td>• Build KRI dashboards</td>
</tr>
<tr>
<td></td>
<td>o Unemployment rates</td>
</tr>
<tr>
<td></td>
<td>o Interest rates</td>
</tr>
<tr>
<td></td>
<td>o Consumer spending/ CPI</td>
</tr>
<tr>
<td></td>
<td>o Commodity prices</td>
</tr>
<tr>
<td>2. Internal System Information</td>
<td>Risk Owner Monitoring:</td>
</tr>
<tr>
<td>• Cybersecurity Risk</td>
<td>• Firewall system report</td>
</tr>
<tr>
<td></td>
<td>• Penetration attack volumes</td>
</tr>
<tr>
<td></td>
<td>• 24/7 monitoring diagnostics</td>
</tr>
<tr>
<td>3. Internal Manual Information</td>
<td>Risk Owner Monitoring:</td>
</tr>
<tr>
<td>• Physical Security Risk</td>
<td>• Property inspection routine/ polling</td>
</tr>
<tr>
<td></td>
<td>• Security Alarms</td>
</tr>
<tr>
<td></td>
<td>• Video Surveillance</td>
</tr>
</tbody>
</table>
Continuous Information Flow

ERM IS JOURNEY, NOT A DESTINATION

We prescribe the A.I.M. Technique:
• Assess
• Implement
• Monitor

The end goal is continuous information flow throughout the ERM Infrastructure

KEY ACTIVITIES
- Annual risk assessment
- Management requests
- Special projects
- Agreed-upon action plans
- Risk mitigation
- Industry-specific best practices

INPUTS
- Business objectives
- Business strategy
- KPIs
- Enterprise risks
- Process risks

PROTECT VALUE BY MANAGING RISK
ERM – Critical Success Factors

Value propositions from a mature ERM process:

**Ownership**
Risk owners are assigned and understand their responsibility for management, oversight and assurance.

**Assurance**
Stakeholders are assured that risk is being managed within the organization’s risk tolerance and receive information regarding the quality and type of control in place.

**Oversight & Responsibility**
Critical risks facing the organization have been identified, managed and reported on a level and frequency that support the organization’s risk tolerance.

**Visibility**
Management has clear view of their risk universe utilizing dashboards showing monitoring controls and residual risk with an actionable playbook ready to execute.
Questions?