

## Enterprise Risk Management in Government Entities

**Angela M. Gillis, CPA, CFSA**  
Manager, Internal Audit and Risk Advisory Services

Schneider Downs & Co., Inc.  
October 19, 2011



## Agenda

- Enterprise Risk Management (ERM) Overview
- Industry vs. Government Sector
- Leading Practices of Enterprise Risk Management
- Pitfalls and Possibilities
- The GAO Risk Management Framework
- Regulatory Information
- Risk Manager Competencies
- Where to Start?
- Implementing Your ERM Function

2

**SCHNEIDER. DOWNS**  
INTEGRITY • INNOVATION • INSPIRATION

## What is Your Risk Management Approach?

3

**SCHNEIDER. DOWNS**  
INTEGRITY • INNOVATION • INSPIRATION

## Enterprise Risk Management (ERM) Overview

**COSO** – The Committee of Sponsoring Organizations of the Treadway Commission


The **COSO** "Enterprise Risk Management-Integrated Framework" defines ERM as ...

"A process, effected 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."

4



**SCHNEIDER. DOWNS**  
INTEGRITY • INNOVATION • INSIGHT





## Enterprise Risk Management (ERM) Overview

- ERM is a success story
  - 93 percent of organizations with formalized ERM programs in place make better risk-informed decisions—a recognized competitive advantage over those that do not have an ERM program (RIMS Survey, 2009).
  - ERM leaders surveyed identified opportunities of ERM to be the adoption of risk management, improved operations, and cultural understanding of the importance of sustaining high credibility (RIMS Survey, 2009)



5



**SCHNEIDER. DOWNS**  
INTEGRITY • INNOVATION • INSIGHT





## Enterprise Risk Management (ERM) Overview

- ERM as a discipline is relatively new
- Management of risk is not new
- Managing risks through a framework
- Chief Risk Officer (CRO)
- A process
  - Identification of the universe of risks
  - Assignment of ownership to risks
  - Active management of these risks
  - Independent monitoring of risks

ENTERPRISE



MANAGEMENT

6



## Enterprise Risk Management (ERM) Overview

RISKS	
Financial Capture and Reporting	Market/Price
Operational/Transaction	Legal/Regulatory Compliance
Entity Culture	Reputation
Technology	Vendor/Sub-contractor
Liquidity	Fraud
Organizational Strategy	External Competitors/Economy/Innovations
Interdependency on Other Business Units	

7



## Industry vs. Government Sector

Inherent differences between risk management approaches:

Industry	Government
Profit Delivery	Delivering Services
Shareholder Value	Stakeholder Value
Linking Risk to Business Strategy	Linking Risk to Public Policies
Continuity of Leadership	Election Process

8

**SCHNEIDER. DOWNS**  
INTEGRITY • INNOVATION • INSPIRATION




### Evolution of Enterprise Risk Management (ERM)

- Original COSO Pyramid
  - Five components
  - All levels of the organization



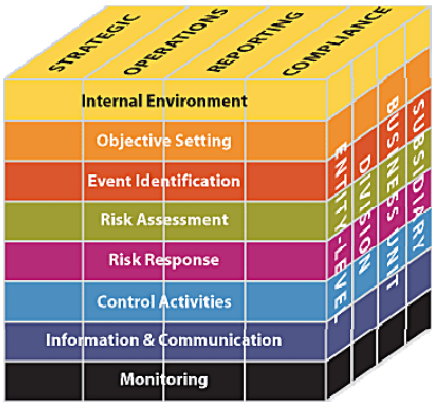
9

**SCHNEIDER. DOWNS**  
INTEGRITY • INNOVATION • INSPIRATION







### Evolution of Enterprise Risk Management (ERM)

- COSO ERM Cube
  - Eight components
  - Four categories
  - All levels of the organization



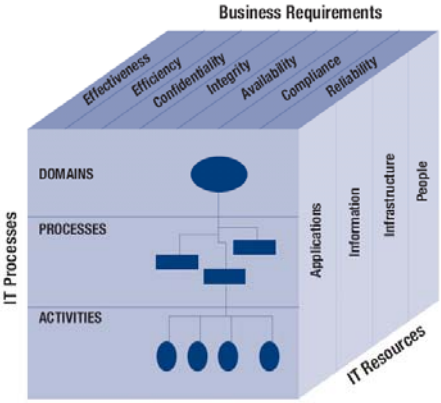
9

10











## Evolution of Enterprise Risk Management (ERM)

- CobiT
  - IT framework
  - Reference process
    - model and common language
  - Control objectives
  - Measure performance
  - Maturity model




11
11











13
12



INTEGRITY • INNOVATION • INSPIRATION

## Leading Practices of Enterprise Risk Management (ERM)

- Fully engaged board of directors
- Integration of risk management into the business functions
- Risk ownership by key management
- Transparency
- Integration of risk with strategic planning
- Intelligence gathering (benchmarking, trend analysis)
- Continuous monitoring (data analytics)
- Scenario analysis (stress testing, disaster recovery)
- Consistent and continuous communication

13
13



INTEGRITY • INNOVATION • INSPIRATION






## Pitfalls and Possibilities

- Pitfalls
  - Not positioning ERM as a management practice
  - Procedural approach (restrictive/limiting)
  - Diminishing transparency
  - Lack of support at the executive level
  - Competing priorities of ERM staff
- Possibilities
  - Integrating risk
  - Focus on systemic risk
  - Focused, intelligent deliberation
  - Increasing public value
  - Fewer surprises
  - Alignment of risk with agency/program goals and objectives



14
14



## The GAO Risk Management Framework

- Developed 2005
- Using several resources
  - Government Performance and Results Act
  - The Government Auditing Standards
  - ERM approach of COSO
  - GAO's Standards for Internal Control in the Federal Government
  - Other
- Strategic planning through implementation and monitoring
- Used to inform
- Designed to be flexible

15



## The GAO Risk Management Framework



The phases contained in the GAO framework are:

**Strategic goals, objectives, and constraints:** Addresses what the strategic goals are attempting to achieve and the steps needed to attain those results.

**Risk assessment:** Addresses identification of key elements of potential risks so that countermeasures can be selected and implemented to prevent or mitigate their effects.


**Alternatives evaluation:** Addresses the evaluation of alternative countermeasures to reduce risk being considered with associated costs.

**Management selection:** Addresses where resources and investments will be made based on alternatives evaluation and other management criteria, such as availability of funds.




**Implementation and monitoring:** Addresses how countermeasures will be applied and the mechanism to keep security measures updated.

Source: Government Accountability Office, Report # GAO-09-687

16




INTEGRITY • INNOVATION • INSPIRATION






## Regulatory Information




- Federal Manager's Financial Integrity Act (FMFIA), 1982
  - Effective and efficient operations
  - Compliance with applicable laws and regulations
  - Reliable financial reporting
  
- OMB Circular A-123, "Management's Responsibility for Internal Controls"
  - Reliable financial reporting



17




INTEGRITY • INNOVATION • INSPIRATION

## Risk Manager Competencies

- The Federal Risk Manager Core Competency Survey
  - Survey of ERM leaders – RIMS
  - Findings
    1. Leadership Experience and Resources
    2. ERM Scope and Standardization
    3. Subject-Matter Awareness
    4. ERM Opportunities and Challenges
    5. Strategic Planning
    6. Skill Assessment



18



INTEGRITY • INNOVATION • INSIGHT






## Risk Manager Competencies




- Finding 1: Leadership Experience and Resources
  - Supervisors with 2-5 years experience in current role
  - 2-10 years experience in risk management, internal controls, auditing or financial management
  - Role = being a sponsor
  - Leading high-level strategic workshops
  - 2-5 staff members for execution



19



INTEGRITY • INNOVATION • INSIGHT

## Risk Manager Competencies

- Finding 2: ERM Scope and Standardization
  - ERM span across a single program or cuts across the entire agency
  - COSO ERM Framework
- Finding 3: Subject-Matter Awareness
  - Beneficial resources identified:
    - Sarbanes-Oxley Act
    - OMB Circular A-123
    - Federal Manager's Financial Integrity Act (FMFIA)
    - CFO Act
    - GAO Internal Control Management and Evaluation Tool
    - GAO Standards for Internal Control

20



**SCHNEIDER DOWNS**  
INTEGRITY • INNOVATION • INSPIRATION

## Risk Manager Competencies

- Finding 4: ERM Opportunities and Challenges
  - Opportunities:
    - Adoption of risk management
    - Improved operations
    - Cultural understanding
  - Challenges:
    - Convincing managers
    - Insufficient executive sponsorship
    - Perception of added burden
    - Providing the appropriate platform

21




**SCHNEIDER DOWNS**  
INTEGRITY • INNOVATION • INSPIRATION




## Risk Manager Competencies

- Finding 5: Strategic Planning
  - Strategic tools
    - Change Management Plan
    - Communication Plan
    - Training and Education Plan
    - Inter-agency collaborative workshops
- Finding 6: Skill Assessment
  - ERM leaders would benefit from additional knowledge and training in:
    - Risk analysis
    - Risk financing
    - Risk management information systems
    - Project risk management


22




INTEGRITY • INNOVATION • INSPIRATION




## Where to Start?



23



INTEGRITY • INNOVATION • INSPIRATION






## Where to Start?

**Which Framework do you use?**

- Anyone you want
- The RIMS Risk Maturity Model (RMM) for ERM assessment:
  - “the key to successful ERM practice depends on the level of maturity the organization demonstrates in seven behavioral attributes:”
    1. Adoption of an ERM-based approach
    2. ERM process management
    3. Risk appetite management
    4. Root cause discipline
    5. Uncovering risks
    6. Performance management
    7. Business resiliency and sustainability

24



## Implementing Your ERM Function

**1**

**Phase 1  
Project governance**

Develop project plan  
Assign executive sponsor  
Define leadership team  
Approval of risk framework  
Other

**2**

**Phase 2  
Conduct the initial enterprise-wide risk assessment & develop an action plan**

Define risk universe  
Develop and define ranking criteria  
Risk assessment advance communication sent to management

**3**

**Phase 3  
Inventory the existing risk management strategies and controls**

Conduct executive interviews – data gathering and documentation  
Evaluate management’s responses on risk  
Perform gap analysis


**4**

**Phase 4  
Reporting and Sustainability**

Develop initial risk reporting  
Develop ongoing monitoring  
Final Plan to organization management  
Develop appropriate executive management & board communications

Key Outputs	Project Plan	Risk workshop advance prep Ranking criteria Standard templates	Completed risk model Gap analysis	Risk reports
-------------	--------------	--	--------------------------------------	--------------


25




## Implementing Your ERM Function

**Phase 1: Project Governance**

- Establish a Risk Office or ERM Office
- Have a dedicated risk champion with good communication skills
- Decide upon the framework
- Develop a project plan
- Establish short and long-term strategic plans
- Collaborate across other agencies
- Don't reinvent the wheel
- Have experienced staff
- Establish an ERM lexicon
- Establish a communications plan



26




## Implementing your ERM Function

**Phase 2: Initial Enterprise Wide Risk Assessment**


- Hold top-down conversations
  - Government agency leaders and key stakeholders
  - Top 10 to 15 risks likely to threaten mission critical objectives
- Determine categories of issues representing key risks (risk universe)
  - Likely to affect the organization key strategic initiatives
  - Many risks may impact an initiative
  - Develop a systemic approach
- Develop and define risk ranking criteria
  - Assigned responsibility
- Define and communicate tolerance of risk
  - Employees and contractors
  - Flow seamlessly and blamelessly

27

Miss-communication or non-communication can cause improper results, blame-throwing and reputational risk

28




## Implementing Your ERM Function

- **Risk Measurement**
  - Probability/Likelihood
    - Prior instances, prevalence and other factors, including volume of transactions and complexity, and number of people involved in the process should be considered - assess each fraud type on its own merits
      - 1) Remote
      - 2) Reasonably possible
      - 3) Probable
  - Severity/Impact
    - Should include financial, monetary, operational, reputational as well as criminal, civil and regulatory liability considerations - assess each fraud type on its own merits




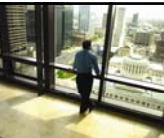
14

29



High S E V E R I T Y  Low	<i>Medium Risk</i>	<i>High Risk</i>
	<i>Share</i>	<i>Mitigate &amp; Control</i>
	<i>Low Risk</i>	<i>Medium Risk</i>
	<i>Accept</i>	<i>Control</i>
	<b>PROBABILITY</b>	High

30





## Implementing Your ERM Function

Risk Assessment Deliverable – Risk Rating Matrix

**Risk Rating Matrix**

Likelihood					
Impact	Rare	Unlikely	Possible	Likely	Almost certain
Catastrophic	moderate	moderate	high	critical	critical
Major	low	moderate	moderate	high	critical
Moderate	low	moderate	moderate	moderate	high
Minor	very low	low	moderate	moderate	moderate
Insignificant	very low	very low	low	low	moderate

17
31


## Implementing Your ERM Function

Risk Assessment Deliverable - Process Control Document

Process Name and Owner	Process Name	Executive responsible
<b>Suppliers/Providers</b>	<b>Process Description</b>	<b>Customers/Users</b>
<ul style="list-style-type: none"> <li>List (and describe) key suppliers</li> </ul>	Describe the process in as much detail as necessary, identifying objectives of the process, procedures in place, how systems operate and interact, key risks and control activities	<ul style="list-style-type: none"> <li>List those who benefit or use information from this process</li> </ul>
<b>Inputs</b>		<b>Outputs</b>
<ul style="list-style-type: none"> <li>List materials, reports, or other relevant inputs</li> </ul>		<ul style="list-style-type: none"> <li></li> </ul>
<b>Key Applications</b>	<b>Policies Governing Process</b>	<b>Significant Accounts Impacted by Process</b>
<ul style="list-style-type: none"> <li>Computer programs</li> </ul>		<ul style="list-style-type: none"> <li>General ledger accounts</li> </ul>
<b>Risk</b>	<b>Control Activity</b>	<b>Control Activity Reference</b>
Identify risk	Describe control activity...	XX-#1 (Control short name)
Next identified risk...	Next description...	XX-#2 (Control short name)
Add rows as needed...	Etc.	Etc.
<b>Relevant Assertions</b>	<b>Assertions Met (list control activities or identify deficiencies)</b>	<b>Control Deficiency Reference</b>
Completeness (for example)	Document what controls provide reasonable assurance that this assertion is met, or describe the control deficiency	OBS-#1 (Deficiency short name)
Next assertion	Next description...	OBS-#2 (Deficiency short name)
Add rows as needed...	Etc.	Etc.

17
32





**SCHNEIDER DOWNS**  
INTEGRITY • INNOVATION • INSPIRATION

## Implementing Your ERM Function

**Phase 3: Inventory existing risk management strategies and controls**

- Data gathering and documentation
- Evaluate management's responses to risk
- Engage the managers of risk
  - Seek diverse perspectives
- Risk Ranking – Impact and Likelihood
- Perform gap analysis
  - Align identified business risks with known controls

35



**SCHNEIDER DOWNS**  
INTEGRITY • INNOVATION • INSPIRATION

## Implementing Your ERM Function

**Phase 4: Reporting and Sustainability**

- Develop risk reporting
- Develop ongoing monitoring
- Development of final plan and framework
- Develop appropriate executive management and board communications



36



INTEGRITY • INNOVATION • INSPIRATION






## Key Takeaways



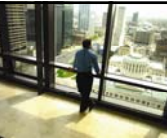
- Understand your organization's culture, strategies and objectives
- Determine a framework to be used
- Communicate constantly and consistently
- Document, document, document
- Training
- Monitoring and reporting



37



INTEGRITY • INNOVATION • INSPIRATION

## Key Takeaways

Thoughts to Ponder ...

- *“The test in the real world is how competent the organization's risk management practices are, and the degree to which [organizations are] instilling risk management behaviors into its culture and management's decision-making [process]. In short, how mature is the company's enterprise risk management program and how thorough are its' practices at all levels of the organization?”*
- *“The key to successful enterprise risk management practices depends on the behavioral attributes of the organization at all levels.”*

*RIMS, 2009*

38

**SCHNEIDER DOWNS**  
INTEGRITY • INNOVATION • INSPIRATION



HARDIN

"We've considered every potential risk except the risks of avoiding all risks."

39

**SCHNEIDER DOWNS**  
INTEGRITY • INNOVATION • INSPIRATION

**Angela M. Gillis**  
Internal Audit and Risk Advisory Services  
CPA, CFSA

**Contact Information:**  
[agillis@schneiderdowns.com](mailto:agillis@schneiderdowns.com)  
Phone: 614-586-7209

41 S. High Street  
Suite 2100  
Columbus, OH 43215

48