



Enterprise Risk Management

Jonelle Pianta, Chief Risk Officer

Overland Park, KS | December 8, 2017

Overview

- What it is and why do it
- Internal ERM
- Auditing ERM





Enterprise Risk Management

What it is and why we should do it

Risks are everywhere

- GSA scandal
- VA scandal
- OPM data breach
- 2016 hurricanes and wild fires
- 2008 financial crisis
- IRS screening of politically active exempt orgs

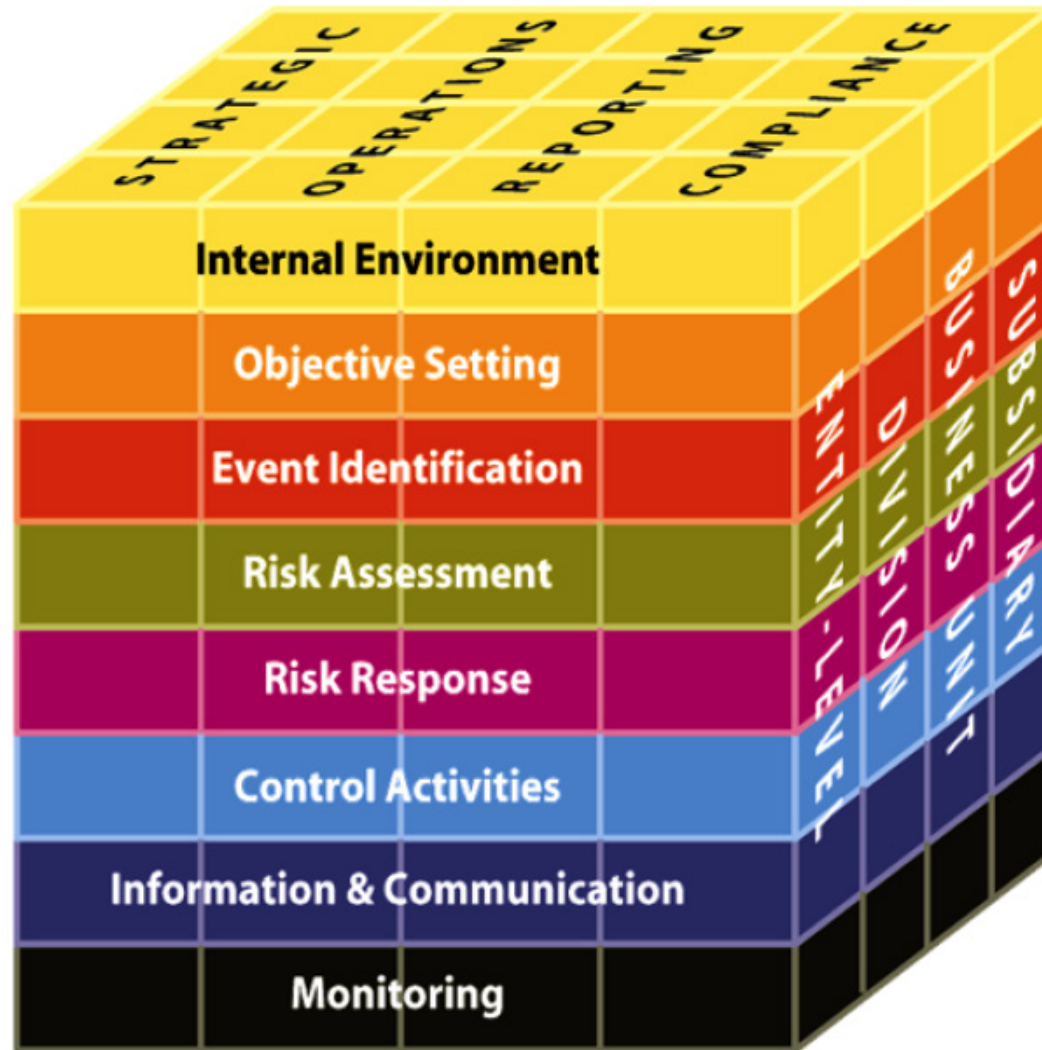


Opportunities are everywhere

While 2017 FEVS results are very positive, survey responses also show several key aspects of Federal workplaces could be improved. Based on employee perspectives, agencies would be more effective to the extent that leaders are able to address insufficient resources, recruit for the right skills, recognize employee performance, and generate commitment and motivation in the workforce.

The results of the survey tell an important story. While multiple aspects of Federal workplaces support effective government, there are always opportunities for improvement. FEVS results point the way to stronger workplaces. The ongoing actions of Federal leadership and employees are key to ensuring that we build on the positive gains we have made over the last few years, while addressing areas in need of improvement.





Trademark by COSO ERM Framework coso.org

ENTERPRISE RISK MANAGEMENT



 **Governance & Culture**

 **Strategy & Objective-Setting**

 **Performance**

 **Review & Revision**

 **Information, Communication, & Reporting**

COSO ERM Framework – Trademark by coso.org



Mandated by OMB A-123

- Revised July 15, 2016
- All Federal agencies effectively manage risks to meet strategic objectives
- Coordinate ERM, strategic planning, strategic review process, and internal control processes



ERM is

- The **culture** and practices that organizations rely on to manage risk in creating, preserving, and realizing public value.
- It will identify potential risks and **opportunities** that could impact how well we achieve our mission, vision, and strategic goals and objectives.



working on the business



Why we do it...

- Advance opportunity
 - Improve mission delivery
 - Reduce costs
 - Focus our corrective actions
- Prioritization – if all risks are important, none are
- Better decision making
- Gain knowledge to review your agency



What ERM is not...

- It does not replace internal controls; it feeds, shapes, and guides them.
- Are you already doing great? It may just be a way to do better.
- It is not a cure-all. Bad stuff will still happen.





Enterprise Risk Management

Internal ERM

How we do it...

- Develop the framework
- Create a risk register
- Evaluate risks
- Risk council ranks the risks for the organization
- Affected offices implement corrective actions
- Evaluate and repeat





Enterprise Risk Management

External ERM

How we do it...

- Develop the framework
 - Who does what
 - Timing
- Evaluate risks
- Rank the risks for the agency
- Evaluate current risks and continue to find new risks



Tips

- Get support from the top
- Sell people on the benefits first so it doesn't become a compliance exercise
- Use plain language
- You don't know how to do it until you do it



ERM feeds governance and decision making – the process is fair and supportable and what is determined to be most important is based on what is best for the organization as a whole.





Questions?

www.hudoig.gov