## Agenda

<table>
<thead>
<tr>
<th>Panelist</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Sallyanne Harper, AFERM</td>
<td>High level review of federal enterprise risk management (ERM).</td>
</tr>
<tr>
<td>2 Tom Brandt, IRS</td>
<td>Review of Internal Revenue Service’s risk profiling processes, including risk identification, categorization, assessment, quantification, measurement, and modeling</td>
</tr>
<tr>
<td>3 Mike Wetklow, NSF</td>
<td>National Science Foundation Implementation – explain risk appetite as a part of risk profiling and what information about remote but severe impact events might be useful to external stakeholders.</td>
</tr>
<tr>
<td>4 Daniel Fodera, FHWA</td>
<td>Federal Highway Administration implementation – explain the tools used in ERM risk profiling, including the use of a heat map.</td>
</tr>
<tr>
<td>5 Board Member</td>
<td>Questions</td>
</tr>
</tbody>
</table>

Note – panelist bios are available in TAB A
Federal Enterprise Risk Management
Sallyanne Harper

Federal Accounting Standards Advisory Board
February 21, 2018
“Life, business, everything you do, every decision you make – it’s all about risk and reward!”

~ Bill Kaplan, founder /leader of the MIT Blackjack Team that won millions in Vegas; inspired the movie 21 and the national bestseller, Bringing Down the House.
## Risk and Risk Management

<table>
<thead>
<tr>
<th>RISK</th>
<th>Risk Management</th>
<th>Enterprise Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Effect of Uncertainty on Objectives</td>
<td>Coordinated effort to manage threats to achieving the organization's goals and objectives</td>
<td>Enterprise wide, systematic approach to managing the portfolio of risks and seizing opportunities related to the achievement of objectives</td>
</tr>
</tbody>
</table>
What is Enterprise Risk Management?

“A discipline that addresses the full spectrum of an organization’s risks, including challenges and opportunities, and integrates them into an enterprise wide, strategically aligned portfolio view. ERM contributes to improved decision-making and supports the achievement of an organization’s mission, goals and objectives.”
1. Events that lead to positive impacts are opportunities

2. Events that lead to negative impacts are threats

3. Events may or may not be risky or controllable
Risk Attributes

1. The scenario describing events leading to a negative or positive impact

2. The likelihood the scenario will occur

3. The consequences of the scenario, should it occur

Source: ISO 31000
But Don‘t We Already Manage Risk?

Typical Risk Management

- Often reactive and not strategically driven
- Typically conducted within functional or program silos.
- Inconsistently applied across the organization

ERM Seeks to ensure:

- Strategic alignment: Mission, Goals, and Objectives
- Comprehensive coverage; a portfolio approach
- Consistent principles and assessments across the organization.
OMB View of A-123 (Internal Controls) and Enterprise Risk Management (ERM)

Risks and Uncertainty
- Strategic
- Operational
- Reputational
- Financial
- Etc.

Strategic Decisions (OMB A-11)
- Mission/Vision
- Goals/Objectives
- Strategic Planning

Budget Decisions (OMB A-11)
- Policy
- President’s Budget
- Congressional Justification

Program Management (OMB A-11)
- Agency Priority Goals
- Cross Agency Priority Goals
- Fed Stat

CXO/Operations Support (OMB A-123)
- Operational Control Objectives
- Reporting Control Objectives
- Compliance Control Objectives
- Risk Assessments
A-123 ERM Implementation Requirements

Establish ERM Governance

Establish a Risk Profile

Integrate with Management Assurance of Internal Controls
The categorization of an entities’ objectives provides for a focus on the separate aspects of Enterprise Risk Management (ERM) and Internal Controls.

Internal Controls are more focused on compliance and reporting while Enterprise Risk Management is more focused on strategy.

The distinct but overlapping category of operations is typically the responsibility of both Internal Controls and Enterprise Risk Management.

Source: Office of Management and Budget Presentation
## Target Operating Model - ERM Integration

### Strategy
- Objective alignment
- Risk Appetite & Tolerance informs mission priorities
- Root cause identification
- Enterprise view of common risk, objectives and potential mitigation strategies
- Opportunities to collaborate

### Performance
- Measurement and monitoring of progress against goals and Risk Appetite & Tolerance
- Risk monitoring of mitigation strategies and investments to validate effectiveness
- KRI monitor emerging risks
- Risk forecasting and stress testing
- Budget

### Budget
- Investments are driven by strategic investment criteria and risk mitigation strategies
- Integrated governance structure drives decisions
- Performance objectives defined

### Capital
- Strategic Initiatives Identified
- Integrated governance structure drives decisions
- Investment criteria, KPIs and KRI monitor emerging risks
- Includes human, IT, and infrastructure investment prioritization

Source: Larry Koskinen, HUD CRO
Essential Elements of Enterprise Risk Management (ERM)

- Align ERM process to goals and objectives
- Identify Risks
- Assess Risks
- Select Risk Response
- Monitor Risks
- Communicate and Report on Risks

Source: GAO. | GAO-17-63
Essential Elements of ERM (GAO)

- Align ERM process to goals and objectives
- Communicate and Report on Risks: Communicate risks to stakeholders and report on the status of addressing the risk.
- Ensure the ERM process maximizes the achievement of agency mission and results.
- Identify Risks: Assemble a comprehensive list of risks both threats and opportunities that could affect the agency from achieving its goals and objectives.
- Monitor Risks: Monitor how risks are changing and if responses are successful.
- Select the response (based on risk appetite) acceptance, avoidance, reduction, share/transfer, or maximize opportunity.
- Assess Risks: Examine risks considering both the likelihood of the risk and the impact of the risk on the agency mission.

Source: GAO | GAO-17-63
COSO ERM FRAMEWORK AND KEY Principles

ENTERPRISE RISK MANAGEMENT

MISSION, VISION & CORE VALUES

STRATEGY DEVELOPMENT

BUSINESS OBJECTIVE FORMULATION

IMPLEMENTATION & PERFORMANCE

ENHANCED VALUE

Governance & Culture
1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting
6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance
10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision
15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

Information, Communication, & Reporting
18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Source: COSO, Enterprise Risk Management-Integrating with Strategy and Performance, September 2017
Applying enterprise risk management to environmental, social and governance-related risks

Figure 1. Evolving risk landscape 2008-2018

<table>
<thead>
<tr>
<th>Top 5 Global Risks in terms of likelihood</th>
<th>2008</th>
<th>2013</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset price collapse</td>
<td>Severe income disparity</td>
<td>Extreme weather events</td>
<td></td>
</tr>
<tr>
<td>Middle East instability</td>
<td>Chronic fiscal imbalances</td>
<td>Natural disasters</td>
<td></td>
</tr>
<tr>
<td>Failed and failing states</td>
<td>Rising greenhouse gas emissions</td>
<td>Cyberattacks</td>
<td></td>
</tr>
<tr>
<td>Oil and gas price spike</td>
<td>Water supply crises</td>
<td>Data fraud or theft</td>
<td></td>
</tr>
<tr>
<td>Chronic disease, developed world</td>
<td>Mismatch of population ageing</td>
<td>Failure of climate-change mitigation and adaptation</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Top 5 Global Risks in terms of impact</th>
<th>2008</th>
<th>2013</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset price collapse</td>
<td>Major systemic financial failure</td>
<td>Weapons of mass destruction</td>
<td></td>
</tr>
<tr>
<td>Retrenchment from globalization (developed)</td>
<td>Water supply crises</td>
<td>Extreme weather events</td>
<td></td>
</tr>
<tr>
<td>Slowing Chinese economy (&lt;6%)</td>
<td>Chronic fiscal imbalances</td>
<td>Natural disasters</td>
<td></td>
</tr>
<tr>
<td>Oil and gas price spike</td>
<td>Diffusion of weapons of mass destruction</td>
<td>Failure of climate-change mitigation and adaptation</td>
<td></td>
</tr>
<tr>
<td>Pandemics</td>
<td>Failure of climate-change mitigation and adaptation</td>
<td>Water crises</td>
<td></td>
</tr>
</tbody>
</table>

Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the World Business Council for Sustainable Development (WBCSD).

Preliminary Draft, January 2018
RISK GOVERNANCE DASHBOARD

NUMBER OF MEETINGS

NUMBER OF RISKS IDENTIFIED

A FEW

LOADS

WEIGHT OF RISK REPORTS

AUDIT OVERKILL

LOW

HIGH

WELL, THAT'S ALL RIGHT THEN
Enterprise Risk Management – Briefing for Federal Accounting Standards Advisory Board
February 2018
Background on IRS’s ERM Program

The IRS Implemented ERM to:

• Determine what risk areas could negatively affect the ability of the Service to carry out its mission
• Identify resources, processes, policies and procedures for proactively managing risk
• Create greater risk management awareness at all levels of the organization
• Provide a coordinated and common framework for capturing and reporting risk information and sharing and reporting risk mitigation efforts
IRS ERM Governance Model

The ERM Governance Model serves as the method in which enterprise risks are discussed amongst executive management. The Governance Model also serves as the method in which decisions will be made relating to those enterprise risks.

IRS Commissioner

- Sets “tone at the top” for risk related collaboration and transparency
- Meets with Executive Risk Committee periodically to discuss enterprise risks
- Key consumer of risk information, and uses risk information as an input to certain decisions

Executive Risk Committee (ERC)

- Chaired by CRO, meets regularly
- Membership includes (9 voting members and 1 non-voting (General Legal Services)):
  - Permanent - CRO, Deputy Commissioners, and Chief Counsel
  - Rotational - 5 Units
  - Invitational - Risk or initiative driven
- Accountable for enterprise level or significant risks (e.g., Strategic / Reputational)
- Provides transparency / recommendations to the Commissioner & input / guidance to the Risk Working Group
- Monitors the enterprise risk register (e.g., evaluates relationships of risks, assesses emerging risks and sponsors risk mitigation strategies)

Risk Working Group (RWG)

- Led by CRO, meets prior to and post the Executive Risk Committee
- Membership includes representation from across the different units
- Accountable for enterprise risk management processes and execution at the unit level
- Aggregates the overarching enterprise risks across business and functional areas / objectives
- Provides enterprise risk analysis, reporting, and support to the Executive Risk Committee
The purpose of risk assessments is to provide management an opportunity to:

- Identify and evaluate risks in order to understand the significant threats to the achievement of objectives;
- Understand activities already underway to respond to those risks; and
- Identify areas where additional activities may be necessary to adequately respond to those risks in accordance with the organization’s risk appetite.
IRS Enterprise Risk Assessment

- On an annual basis the IRS Office of the Chief Risk Officer (OCRO) facilitates an enterprise risk assessment.
- An initial high-level top-down enterprise risk assessment was conducted in 2014 known as the Temperature Check.
- Building upon this initial assessment, the OCRO designed the approach for the 2015 enterprise risk assessment, and developed a repeatable process to guide the enterprise risk assessments.
- The 2015, 2016, and 2017 risk assessments took more of a bottom-up approach.
  - All units provide business unit risk registers to the OCRO.
    - All risks identified by the business units should be managed and monitored by unit leadership on an ongoing basis.
  - The OCRO aggregates the results and provides some initial reports to the Risk Working Group (RWG), comprised of ERM Liaisons from all IRS units.
  - The RWG analyzes the results from an enterprise perspective and works with OCRO to develop a proposed enterprise risk list.
  - The Executive Risk Committee (ERC) reviews the information from the RWG, determines next steps and assigns accountability.
Example Enterprise Risk Assessment Process and Timeline

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Step 2</th>
<th>Step 3</th>
<th>Step 4</th>
<th>Step 5</th>
<th>Step 6</th>
</tr>
</thead>
</table>
| All units submit:  
• Unit risk registers,  
• Templates indicating whether they believe each of the previous enterprise risks should remain, input on the future outlook of the risks, and any risks they think should be added. | Risk Working Group (RWG) reviews aggregated risk information to:  
• Identify any changes that should be made to enterprise risks,  
• Discuss the future outlook of the risks, and  
• Discuss and agree on the consolidated list of enterprise risks. | Each RWG member meets with their head of office to:  
• Score each enterprise risk, and  
• Indicate which enterprise risks they believe require additional focus over the next year. | Executive Risk Committee meets to:  
• Review initial enterprise risk assessment outputs,  
• Agree on any changes,  
• Review and discuss the future outlook of the risks,  
• Determine which risks require additional focus over the next year, and  
• Assign accountable parties to develop recommendations to address risks. | Accountable parties identified for the risks selected by the Executive Risk Committee for additional focus:  
• Develop recommendations for additional focus, and  
• Develop materials to support presentation of recommendations to the Executive Risk Committee. | Executive Risk Committee meets to:  
• Review additional actions recommended by accountable parties, and  
• Determine associated next steps. |

IRS Risk Assessment Process

Enterprise Risk Assessment Process

Key Inputs

- Business Unit Risk Information Set
- Oversight / Audit Risk and Issue Information Set
- Self Assessments
- Interviews / Focus Groups

Objectives

- Identify Inherent Risk
- Identify Mitigants
- Assess Residual Risk

Prioritization Based on Appetite
Consider each risk category in the context of your unit’s objectives to make sure you are thinking through the full spectrum of risks that may impact your objectives. Reviewing risk categories may help recognize previously unidentified risks.

<table>
<thead>
<tr>
<th>Risk Type</th>
<th>Definition</th>
<th>Risk Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic / Reputational</td>
<td>Aligned with and directly related to the IRS mission</td>
<td>• Mission/Scope</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Trust, Confidence and Reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Customer Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enforcement</td>
</tr>
<tr>
<td>Financial / Reporting</td>
<td>Reliability of the overall financial well-being of the IRS and the U.S. tax system</td>
<td>• Budget</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Tax Fraud</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Administrative Fraud</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Improper Payments</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Tax Complexity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Stewardship of Taxpayer Dollars</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• External Reporting</td>
</tr>
<tr>
<td>Legal / Regulatory</td>
<td>IRS compliance with applicable laws and regulations</td>
<td>• Laws &amp; Regulations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Litigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Taxpayer Rights &amp; Protection</td>
</tr>
<tr>
<td>Operational</td>
<td>Effectiveness and efficiency of the IRS’s operations</td>
<td>• Program/Operational Effectiveness</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Information/Data Reliability &amp; Sufficiency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Management Oversight</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disruption to Operations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Physical Security</td>
</tr>
<tr>
<td>Organizational</td>
<td>Effectiveness of the IRS’s structure, culture, and people</td>
<td>• Human Capital</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Organizational Culture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Morale</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Organizational Structure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Leadership</td>
</tr>
<tr>
<td>Technology</td>
<td>Effectiveness, efficiency and security of the IRS’s technology</td>
<td>• Infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Information Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Technical Effectiveness/Agility</td>
</tr>
</tbody>
</table>
Identifying Changes to Key Internal and External Factors and Considering Impact on Risk Profile

- Monitoring internal and external factors that could create, compound, or reduce risk exposure for your unit allows for a more informed risk profile.
- Consider factors in the external environment across each of the following categories:

<table>
<thead>
<tr>
<th>Categories</th>
<th>Characteristics of External Environment</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Political</td>
<td>The nature and extent of government intervention and influence, including tax policies, labor laws, environmental laws, trade restrictions, tariffs, and political stability</td>
<td>Change in the Administration</td>
</tr>
<tr>
<td>Economic</td>
<td>Interest rates, inflation, foreign exchange rates, availability of credit, etc.</td>
<td>Globalization of the economy</td>
</tr>
<tr>
<td>Social</td>
<td>Stakeholder needs or expectations; population demographics, such as age distribution, educational levels, distribution of wealth</td>
<td>Changing demographics of taxpayers</td>
</tr>
<tr>
<td>Technological</td>
<td>R&amp;D activity, automation, and technology incentives; rate of technological changes or disruption</td>
<td>Increased use of blockchain by financial institutions</td>
</tr>
<tr>
<td>Legal</td>
<td>Laws (e.g., employment, consumer, health and safety), regulations, and industry standards</td>
<td>New legislative requirements</td>
</tr>
<tr>
<td>Environmental</td>
<td>Natural or human-caused catastrophes, ongoing climate change, changes in energy consumption regulations, attitudes toward the environment</td>
<td>Natural disasters impacting IRS operations</td>
</tr>
</tbody>
</table>

- Changes in external factors across any of these categories may have implications for the risks facing your unit.
- Consider how changes have created, compounded, or reduced risk exposure and incorporate this insight into your risk assessment.
Identifying Changes to Key Internal and External Factors and Considering Impact on Risk Profile (Contd.)

- Consider factors in the internal environment across each of the following categories:

<table>
<thead>
<tr>
<th>Categories</th>
<th>Characteristics of External Environment</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy / Structure</td>
<td>Approaches to pursuing goals and objectives, organizational structure</td>
<td>Business unit re-organization</td>
</tr>
<tr>
<td>People</td>
<td>Knowledge, skills, attitudes, relationships, core values, and culture</td>
<td>Change to the percentage of employees who are retirement eligible</td>
</tr>
<tr>
<td>Process</td>
<td>Activities, tasks, policies, or procedures; changes in management, operational, and supporting processes</td>
<td>New process or changes to existing processes</td>
</tr>
<tr>
<td>Technology</td>
<td>New, amended, or adopted technology</td>
<td>New systems or changes to existing systems</td>
</tr>
</tbody>
</table>

- Changes in internal factors across any of these categories may have implications for the risks facing your unit.
- Consider how changes have created, compounded, or reduced risk exposure and incorporate this insight into your risk assessment.
### 2017 Enterprise Risk Summary – SAMPLE RISK OVERVIEW

**Primary Strategic Goal Impacted**

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Critical Staffing Shortages</td>
<td>The risk that increased attrition and continued constraints in hiring and retaining employees with needed skills and expertise results in critical business failures and over-reliance on contractors.</td>
</tr>
</tbody>
</table>

**Relationships with other Enterprise Risks**

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
<th>20</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>5</td>
</tr>
</tbody>
</table>

*If shaded, the risk has the potential to impact that Strategic Goal*

**Strategic Goals**

- **4. Cultivate a well-equipped, diverse, flexible, and engaged workforce**

<table>
<thead>
<tr>
<th>Impact</th>
<th>Likelihood</th>
<th>No</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.50, 4.14</td>
<td>4.17, 3.88</td>
<td>8</td>
<td>14</td>
</tr>
</tbody>
</table>

- **2016 Score**

  - 4.50
  - 4.14

- **2017 Score**

  - 4.17
  - 3.88

**# of Unit Risks Mapped**

- 46
<table>
<thead>
<tr>
<th>Year</th>
<th>Outputs</th>
<th>Outcomes</th>
</tr>
</thead>
</table>
| 2014 | • 15 enterprise risks  
• Likelihood and impact scores | • The units gained transparency into and agreement on the top risks facing the IRS  
• Greater understanding by each unit of how the enterprise risks were potentially affecting their unit.  
• The process enhanced risk awareness and dialogue within and across the units. |
| 2015 | • 29 enterprise risks  
• 6 top enterprise areas of risk  
• Assigned accountable parties for actions for each of 6 top enterprise areas of risk | • All business units have risk registers to actively manage risk to their unit’s objectives.  
• Units have a greater understanding of the various risk management related activities within their organization to better connect elements and fully operationalize risk management.  
• Accountable parties reported to the ERC on mitigating actions taken for the 6 top enterprise areas of risk. |
| 2016 | • 22 enterprise risks  
• Likelihood and impact scores  
• 5 top enterprise risks  
• Assigned accountable parties for the top five enterprise risks | • ERC deliberated and decided upon the top enterprise risks to focus on.  
• ERC reviewed the current response strategies for the top 5 enterprise risks, assigned specific actions, and endorsed an investment as an input to the Senior Executive Team investment decision process. |
| 2017 | • 20 enterprise risks  
• Likelihood and impact scores  
• 5 top enterprise risks  
• Assigned accountable parties for all enterprise risks | • ERC deliberated and decided upon three enterprise risks they would like additional focus given to.  
• More outcomes will likely result as the ERC meets with the accountable parties for the enterprise risks selected for additional focus. |
Key Changes to IRS’s Risk Profile over Time

In 2015, the 6 top enterprise areas of risk were:
- Authentication / Authorization
- Budget
- Cyber Security
- Integrated Strategy and Objectives
- Operational Effectiveness and Efficiency
- Workforce

In 2016, the top 5 enterprise risks were:
- Aging Technology Infrastructure
- Record Retention and Discovery
- Complexity of Cyber Threats
- Specialized Skills and Expertise
- Attrition

In 2017, the top 5 enterprise risks were:
- Aging Technology Infrastructure
- Cyber and Data Security
- Critical Staffing Shortages
- Secure Access to IRS Services
- Data Breaches at External Entities

There have continued to be top risks related to the following area since 2014:
- Workforce
- Budget*

The following areas from 2015 continue to be high ranking risks:
- Cyber Security (Cyber and Data Security)
- Authentication / Authorization (Secure Access to IRS Services)

The following risk from 2016 continues to be a high ranking risk:
- Aging Technology Infrastructure

The following new risks were added for 2017:
- Data Breaches at External Entities
- External Engagement

*Note: There continued to be a top risk related to the budget, but in 2016 and 2017 the ERC decided to capture this with other factors of the IRS’s current environment in a preamble to the Enterprise Risk Profile.
Much has been accomplished with regard to ERM since the Program began in 2014.

- As the risk profile continues to evolve, the IRS has a better understanding of its enterprise risks after completing 4 enterprise risk assessments.

- Each unit has a better understanding of the risks that can have the most impact on achieving its unit objectives and uses a risk register to capture this information.

- Risks are discussed and considered in decision making.

- The Business Performance Review (BPR) process includes discussions of risk.

- The IRS is embracing a more risk-aware culture and considers risks as a part of daily operations. As part of these efforts, over 10,000 senior managers, managers and management officials have been trained on ERM.

- Every unit has made progress toward operationalizing ERM.

The ERM program will continue to evolve as capabilities are further developed, and as risks continue to emerge. The changing external environment for the IRS makes ERM extremely important as it must deal with rapid change and an evolving technology landscape.
Next Presentation
Enterprise Risk Management
Risk Profiling
Federal Accounting Standards Advisory Board Presentation
Mike Wetklow
February 21, 2018
Objective

FASAB Ask: “Explain risk appetite as a part of risk profiling and what information about remote but severe impact events might be useful to external stakeholders.”

This briefing will attempt to meet FASAB’s objective by covering:

1. Background on OMB A-123 and describing NSF’s implementation approach
2. How to demystify risk appetite with broad Agency examples
3. COSO Standards - Risk Appetite Principle

This presentation is made in my personal capacity and the views expressed herein do not necessarily represent the views of DHS, OMB, NSF, or the U.S. Government.
Background on OMB A-123 and NSF Implementation Approach
OMB A123 General ERM Background

- Establish risk management processes to identify problems early, bring them to leadership early, and develop solutions.
- Modernize FMFIA efforts and introduce the relationship between ERM and internal control.
- Integrate governance to improve mission delivery, reduce costs, and focus on key risks.
- Move A-123 beyond CFO function and bring better balance between financial reporting, compliance, and effectiveness/efficiency objectives.
- It's ok to talk about risks and important to work with auditors.
- Risk is not always negative its about opportunities also.

- ERM requirements were limited to establishing an initial risk profile, integration with internal controls and getting better at it over time.
- The concept of risk appetite is key to achieving effective ERM, and is essential to consider in determining risk responses.
## OMB A-123 Risk Profile Example

### STRATEGIC OBJECTIVE – Improve Program Outcomes

<table>
<thead>
<tr>
<th>Risk</th>
<th>Inherent Assessment</th>
<th>Current Risk Response</th>
<th>Residual Assessment</th>
<th>Proposed Risk Response</th>
<th>Owner</th>
<th>Proposed Risk Response Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency X may fail to achieve program targets due to lack of capacity at program partners.</td>
<td>High</td>
<td>High</td>
<td>REDUCTION: Agency X has developed a program to provide program partners technical assistance</td>
<td>High</td>
<td>Medium</td>
<td>Agency X will monitor capacity of program partners through quarterly reporting from partners</td>
</tr>
</tbody>
</table>

### OPERATIONS OBJECTIVE – Manage This Risk of Fraud in Federal Operations

<table>
<thead>
<tr>
<th>Risk</th>
<th>Inherent Assessment</th>
<th>Current Risk Response</th>
<th>Residual Assessment</th>
<th>Proposed Risk Response</th>
<th>Owner</th>
<th>Proposed Risk Response Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract and Grant fraud.</td>
<td>High</td>
<td>Medium</td>
<td>REDUCTION: Agency X has developed procedures to ensure contract performance is monitored and that proper checks and balances are in place.</td>
<td>High</td>
<td>Medium</td>
<td>Agency X will provide training on fraud awareness, identification, prevention, and reporting.</td>
</tr>
</tbody>
</table>
NSF Guiding Principles for Implementing ERM (Based on COSO)

• Support from the Top is a Necessity
• Build ERM Using Incremental Steps
• Focus initially on a Small Number of Top Risks
• Leverage Existing Resources
• Build on Existing Risk Management Activities
• Embed ERM into the Decision Making Practices of the Organization
• Provide Ongoing ERM Updates and Continuing Education for Leadership and Senior Management
How to demystify risk appetite with broad Agency examples
Risk Appetite - Demystified
“DHS manages risk every day, and in an environment of new and evolving threats, we cannot do more with less. As a result, we strive to ensure that the limited resources we have cover our areas of greatest risk before seeking additional resources to meet agency requirements.”
Illustrative NSF Example

“NSF seeks high-risk, potentially transformative projects that will generate pioneering discoveries and advance executing new frontiers in science.”

COSO Framework and Risk Appetite
Principle
COSO’s Enterprise Risk Management Framework - June 2017

1. Governance and Culture
2. Strategy and Objective Setting
3. Performance
4. Review and Revision
5. Information, Communication and Reporting

Strategy & Objective Setting:
- Analyzes Business Context
- Defines Risk Appetite
- Evaluates Alternative Strategies
- Formulates Business Objectives
Risk Appetite

• The organization defines risk appetite in the context of creating, preserving, and realizing value.

• Risk Appetite defined – The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value.
Risk Appetite Key Things to Know

• Applying Risk Appetite
  – Decisions made in selecting strategy and developing risk appetite are not linear, with one decision preceding the other.

• Determining Risk Appetite
  – There is no standard or “right” risk appetite that applies to all entities.

• Articulating Risk Appetite
  – Some organizations articulate risk appetite as a single point; others as a continuum.

• Using Risk Appetite
  – Risk appetite guides how an organization allocates resources, both through the entire entity and in individual operating units.
For More information on Risk Appetite.....


– Just need to be careful translating to new/current COSO framework
THANK YOU, Keep in touch!

www.linkedin.com/in/mikewetklow

https://twitter.com/mikewetklow
Next Presentation
FHWA Risk Management

Risk Management in Practice

Daniel Fodera, CERM
Federal Highway Administration
The international definition of risk is “the effect of uncertainty on objectives.”

Risk is about uncertainty, it is always in the future. It may or may not happen.

Risk is about some effect, positive or negative, it will have an impact

Risk is about objectives, we must know what we are trying to achieve. This can be as an organization, program, or project.
FHWA Mission, Vision, Values

- FHWA Vision: "Our Agency and Our Transportation System are the Best in the World."
- FHWA Mission: "Improve Mobility on our Nation’s Highways Through National Leadership, Innovation, and Program Delivery."
- FHWA Values: "Public Service, Integrity, Respect, Personal Development, Collaboration, and Family."
- Administer $42 Billion annual in Highway Trust funds, providing oversight of approximately 15,000 construction projects each year. 52 Division Offices, 2,300 field and HQ employees. Civil Engineers, Transportation Planners, Finance Managers, Environmental and Civil Rights Specialists, Program and Management Analysts.
Who Manages Risk?
Consider risk at different levels of the organization

- **Agency**
  - Agency level risks are threats or opportunities to the organization’s strategic goals or which involves multiple levels.
  - Responsibility: Senior executives, policy makers

- **Program**
  - Program risks are common to groups of projects that achieve strategic goals.
  - Responsibility: Program managers

- **Project**
  - Project risks are specific to individual projects.
  - Responsibility: Project managers

- **Activity**
  - Activity risks are specific to ongoing functions that support programs or projects.
  - Responsibility: Activity managers
Risk Management Process and Components of Internal Control

- Identify the Risks
- Analyze the Risks
- Evaluate and Prioritize the Risks

Information and Communication

Control Environment

Monitoring Activities

Control Activities

Updated for 2016
<table>
<thead>
<tr>
<th>Risk Management Process Step</th>
<th>Key Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication and Consultation</td>
<td>Who needs to be involved? How will we communicate and consult with them?</td>
</tr>
<tr>
<td>Identify the Context</td>
<td>What program or other objective areas will we assess? What are the things to consider when we assess them? <em>What are the existing controls and how are they working? How do you know?</em> What criteria will we use to assess our risks? Who will do the assessment?</td>
</tr>
<tr>
<td>Identify the Risks</td>
<td>What events could happen that would affect my objectives? What are the corresponding impacts? What are my If...then... statements?</td>
</tr>
<tr>
<td>Analyze– Assess Impact</td>
<td>What is the severity of this impact according to my criteria?</td>
</tr>
<tr>
<td>Analyze– Assess Likelihood</td>
<td>What is the likelihood that this risk event will occur?</td>
</tr>
<tr>
<td>Prioritize Risks</td>
<td>What is the expected value of each risk statement? How do the risks compare? Which risks does leadership consider the “key risks?” Which risks will require a response?</td>
</tr>
<tr>
<td>Plan and Execute Risk Response Strategies</td>
<td>What actions will we take to mitigate, avoid, accept, transfer, or enhance our risks? What actions are important to take now? Who is accountable, when will they start, and when will it be done?</td>
</tr>
<tr>
<td>Monitor, evaluate, and adjust</td>
<td>What is the status of our response actions? Are they completed, in progress, not started, or has the action been deferred? Did the action have the desired effect? What is the residual risk and how should we respond?</td>
</tr>
</tbody>
</table>
Step 3 – Identify The Risks

• Generate a list of risks that answer the key questions.
  – Include known risks from prior assessments, include them.

• The Risk Statements
  – use the “if/then” format to identify the risk events and the resultant impacts.
<table>
<thead>
<tr>
<th>Risk Short Description</th>
<th>Event</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impacts from delayed funding</td>
<td>If funding (CR's, re-statements, transfers) and notifications (Form FHWA-370 and advices) are not received in a timely manner.</td>
<td>Then new projects may not be started and current projects could be delayed; funding opportunities could be lost; payroll processing may be delayed.</td>
</tr>
<tr>
<td>Performance Management</td>
<td>If the Notice of Proposed Rulemaking does not get issued as scheduled</td>
<td>then State DOTs and MPOs will not be able to comply with the law.</td>
</tr>
<tr>
<td>Innovation</td>
<td>If we fail to implement a coordinated Infrastructure research program to identify, promote and implement innovation</td>
<td>we will miss opportunities to leverage all of the resources FHWA has to identify and address emerging needs, and deploy essential technology that will advance our transportation goals</td>
</tr>
<tr>
<td>10-yr PE</td>
<td>If the state does not adhere to 23 CFR 630.112(c)(2), (10-year PE requirements)</td>
<td>then the state may/will be required to pay back significant amount of money.</td>
</tr>
<tr>
<td>Utility-Investigation (Design)</td>
<td>If adequate utility investigation is not performed during design.</td>
<td>Then conflicts will continue to arise during construction which may increase cost and contract time.</td>
</tr>
<tr>
<td>System Changes</td>
<td>If the FMIS modernization implementation, Current Bill System, or E-Travel are delayed or encounter significant issues,</td>
<td>FHWA may not be able to enter funding into FMIS, and states may not be able to obligate funding in a timely manner, reimbursement of allowable expenses may be delayed, and the ability for employees to enter travel and enter travel expense data into the system may be delayed.</td>
</tr>
<tr>
<td>FMIS 5.0 Implementation</td>
<td>If obstacles are encountered during FMIS 5.0 implementation,</td>
<td>then project authorizations may be substantially delayed and project data quality may be inconsistent.</td>
</tr>
<tr>
<td>Billing Risks with FMIS 5.0 and IRIS</td>
<td>If there are not sufficient billing controls in place with transition to FMIS 5.0 and IRIS,</td>
<td>then improper payments may be processed.</td>
</tr>
<tr>
<td>Planning through Construction Obligation</td>
<td>If the links between project planning and construction authorization are not improved,</td>
<td>then projects will continue to be programmed for construction without having completed project development, which leads to delays and increased project costs.</td>
</tr>
<tr>
<td>QA/QC Bonuses</td>
<td>If the State pays excessive amounts of QA/QC bonuses to contractors,</td>
<td>then the QA/QC bonuses become an ineffective tool to achieve the intent of the program and not motivate for higher quality work. Improving the process has the potential to improve relations with the construction industry and to increase the potential for the more competitive contractor to become the successful bidders.</td>
</tr>
</tbody>
</table>
Step 4 – Analyze the Risks

- Impact Assessment
  - Estimate the level of impact based on what will happen if the event occurs.
  - Use the risk impact criteria to inform your assessment.
  - Elect an impact level of insignificant or neutral, minor, moderate, major, or catastrophic.

- Likelihood Assessment
  - Estimate the likelihood an event is to occur based on data or opinion.
  - Certain conditions may increase or decrease the likelihood of a risk event and an impact.
  - Use the risk likelihood criteria in the Appendix to inform your assessment and select a likelihood level of unlikely, possible, likely, or almost certain for each risk.
Communicate and Consult with Stakeholders

Identify

Risk Context

Identify the Risks

Analyze the Risks

Evaluate and Prioritize the Risks

Respond to the Risks

Monitor, Review, and Adjust

Impact Criteria

- Scale
  - Catastrophic
  - Major
  - Moderate
  - Minor
  - Insignificant

- Criteria
  - Financial
  - Reputation
  - Business Operations
  - Legal and Compliance
  - Infrastructure Assets
  - Resources and Effort Required
  - Human and Natural Environment
  - Safety
  - Civil Rights
  - Economic
Likelihood Criteria

**Scale**
- Almost Certain
- Likely
- Possible
- Unlikely

- Staffing (Levels & Experience)
- Operational Procedures
- Guidance
- Problem History
- New Program, Phase or Component
- Complexity
- Outside Control
- Potential for Waste, Fraud & Abuse
- Work Force Development & Training
- FHWA Involvement
- Consultant Use

Risk Assessment

Monitor, Review, and Adjust
Step 5 – Evaluate and Prioritize The Risks

• Use impact and likelihood to determine a relative importance and a priority ranking for the risks.
  – A priority ranking communicates what are the most important issues.

• Key Questions - How do the risks compare? Which risks does leadership consider the “top risks?” Which risks will require a response?

• Outcome - A prioritized list of identified risks.
  – Prioritization and identification of top risks should be informed by the analysis results and validated by leadership
Heat Map Tool

- A graphical plot or visual tool used to represent the relative placement of risks. The expected value of the risk determines its location.
<table>
<thead>
<tr>
<th>Impact</th>
<th>Description</th>
<th>Likelihood</th>
<th>Unlikely</th>
<th>Possible</th>
<th>Likely</th>
<th>Almost Certain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Large unacceptable financial loss, severe budget variance. Very significant harm to image with substantial impact on effectiveness. Large and unacceptable operational impact, long term business interruption. Qualified audit finding.</td>
<td>The event could possibly occur, but is unlikely at this time.</td>
<td>The event could occur under specific conditions and some of those conditions are currently evidenced.</td>
<td>The event is most likely to occur in most circumstances.</td>
<td>The event is expected to occur in most circumstances or is happening now.</td>
<td></td>
</tr>
<tr>
<td>Major</td>
<td>Very significant financial loss, major budget variance. Major embarrassment leading to significant impact on effectiveness. Unacceptable operational impact, short term business interruption. Leads to material weakness.</td>
<td>The event could possibly occur, but is unlikely at this time.</td>
<td>The event could occur under specific conditions and some of those conditions are currently evidenced.</td>
<td>The event is most likely to occur in most circumstances.</td>
<td>The event is expected to occur in most circumstances or is happening now.</td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>Significant financial loss and variance to budget. Moderate embarrassment impacting short term effectiveness. Moderate operational impact, business not interrupted. Leads to reportable findings.</td>
<td>The event could possibly occur, but is unlikely at this time.</td>
<td>The event could occur under specific conditions and some of those conditions are currently evidenced.</td>
<td>The event is most likely to occur in most circumstances.</td>
<td>The event is expected to occur in most circumstances or is happening now.</td>
<td></td>
</tr>
<tr>
<td>Minor</td>
<td>Minor financial loss, small budget variance. Minor embarrassment, but no harm to image or reputation. Minor operational impact, business not interrupted. Leads to audit findings.</td>
<td>The event could possibly occur, but is unlikely at this time.</td>
<td>The event could occur under specific conditions and some of those conditions are currently evidenced.</td>
<td>The event is most likely to occur in most circumstances.</td>
<td>The event is expected to occur in most circumstances or is happening now.</td>
<td></td>
</tr>
<tr>
<td>Insignificant or Neutral</td>
<td>Minimal or no measurable operational impact. Can be managed with routine activities. Leads to immaterial audit findings.</td>
<td>The event could possibly occur, but is unlikely at this time.</td>
<td>The event could occur under specific conditions and some of those conditions are currently evidenced.</td>
<td>The event is most likely to occur in most circumstances.</td>
<td>The event is expected to occur in most circumstances or is happening now.</td>
<td></td>
</tr>
</tbody>
</table>
FHWA Recovery Act Risk Assessment

- Program Delivery (FLH) (Opportunity)
- Eligibility/Improper Payments
- Indian Reservation Roads Program
- Achievement of Program Goals
- Contract Administration
- Quality Assurance
- LPA
- Right of Way
- Environmental
- DBE
- Transparency
- Qualified Personnel
- STIP

Impact vs. Likelihood Matrix:

- Higher impact, higher likelihood
- Higher impact, lower likelihood
- Lower impact, higher likelihood
- Lower impact, lower likelihood
• Unit leadership should review the risk ranking and determine the priority order. This provides a systems perspective to normalize the unit risks across program and performance areas.
• Identify the unit “top risks”
Benefits of Risk Management

• Focus limited resources
• Strengthen the ability to efficiently manage program delivery
• Improve communication and manage risk corporately.
  – Consistent framework to assess, communicate, and act on possible futures.
  – Critical for an innovative, transformational agency
• Oh by the way...2017 marks ten years as top tier best places to work in the federal government (33/339).
  – http://bestplacetowork.org/BPTW/rankings/detail/TD04
Daniel Fodera
Federal Highway Administration
daniel.fodera@fhwa.dot.gov
404-562-3672
BOARD MEMBER