



Federal Accounting Standards Advisory Board

ERM Risk Profiling Education Session

TAB A
February 21, 2018

Agenda

	Panelist	Topic
1	Sallyanne Harper, AFERM	High level review of federal enterprise risk management (ERM).
2	Tom Brandt, IRS	Review of Internal Revenue Service's risk profiling processes, including risk identification, categorization, assessment, quantification, measurement, and modeling
3	Mike Wetklow, NSF	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.
4	Daniel Fodera, FHWA	Federal Highway Administration implementation – explain the tools used in ERM risk profiling, including the use of a heat map.
5	Board Member	Questions

Note – panelist bios are available in TAB A

Federal Enterprise Risk Management

Sallyanne Harper

Federal Accounting Standards
Advisory Board
February 21, 2018

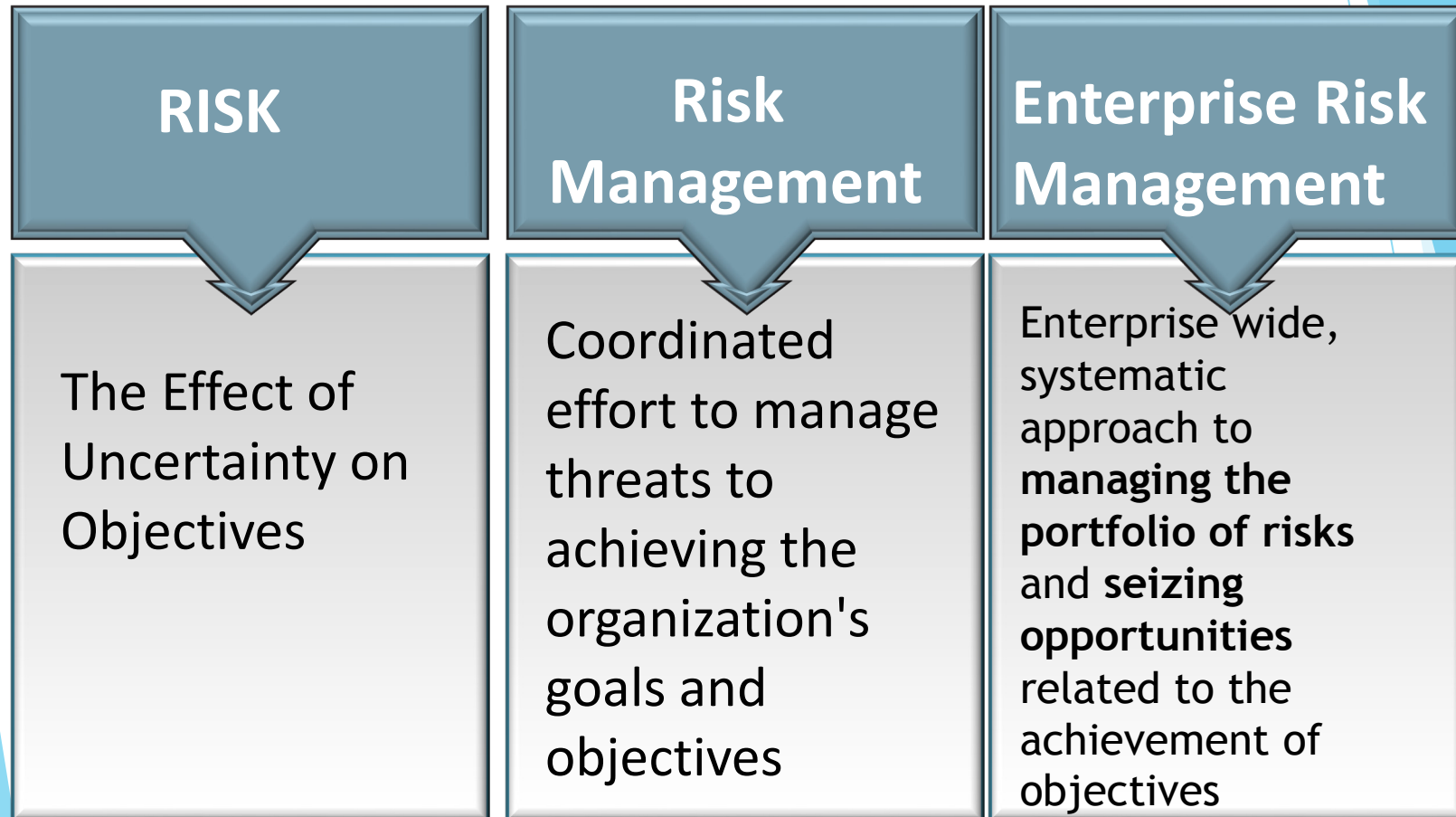


“Life, business, everything you do, every decision you make – it’s all about risk and reward!”

~ 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*.



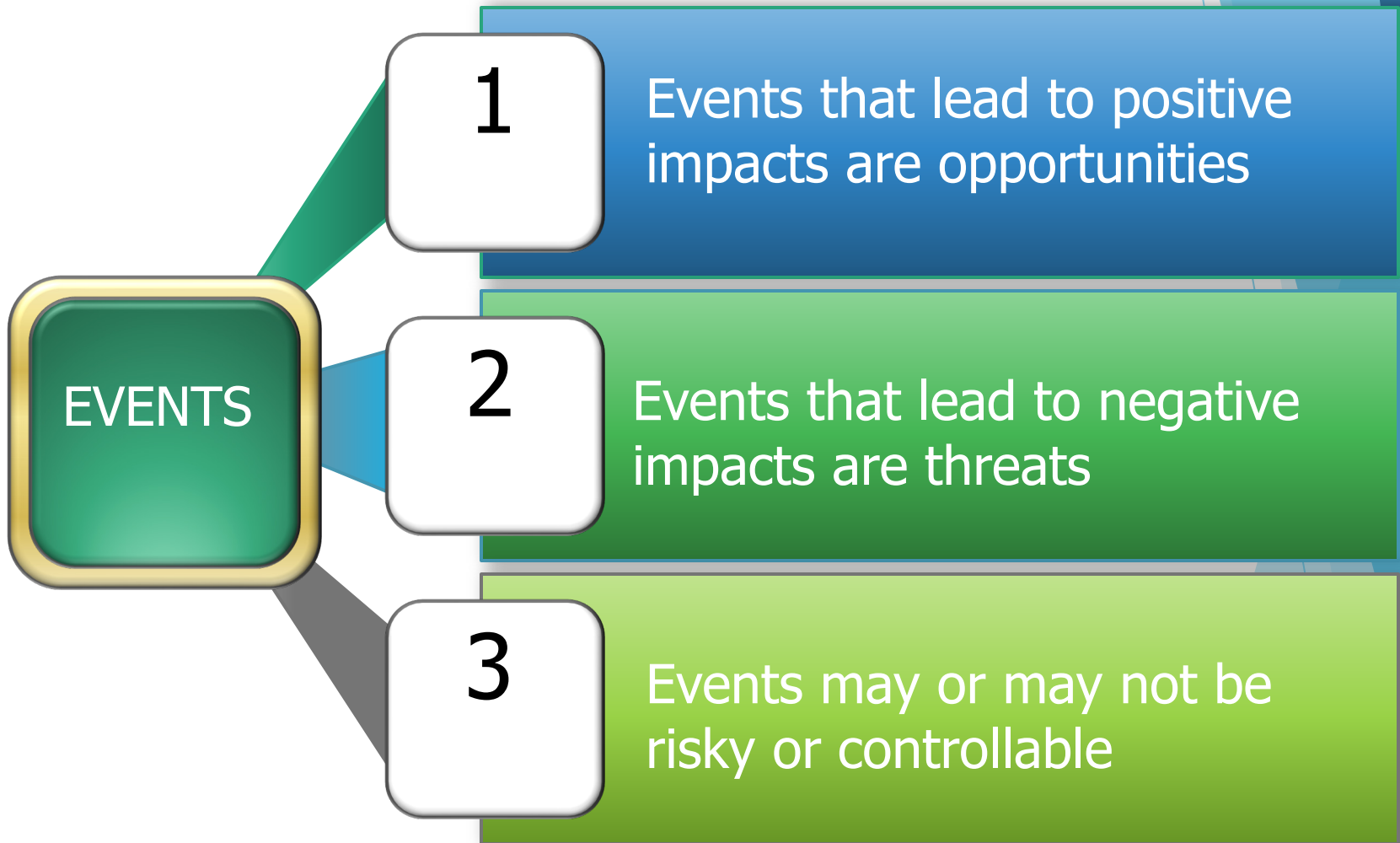
Risk and Risk Management

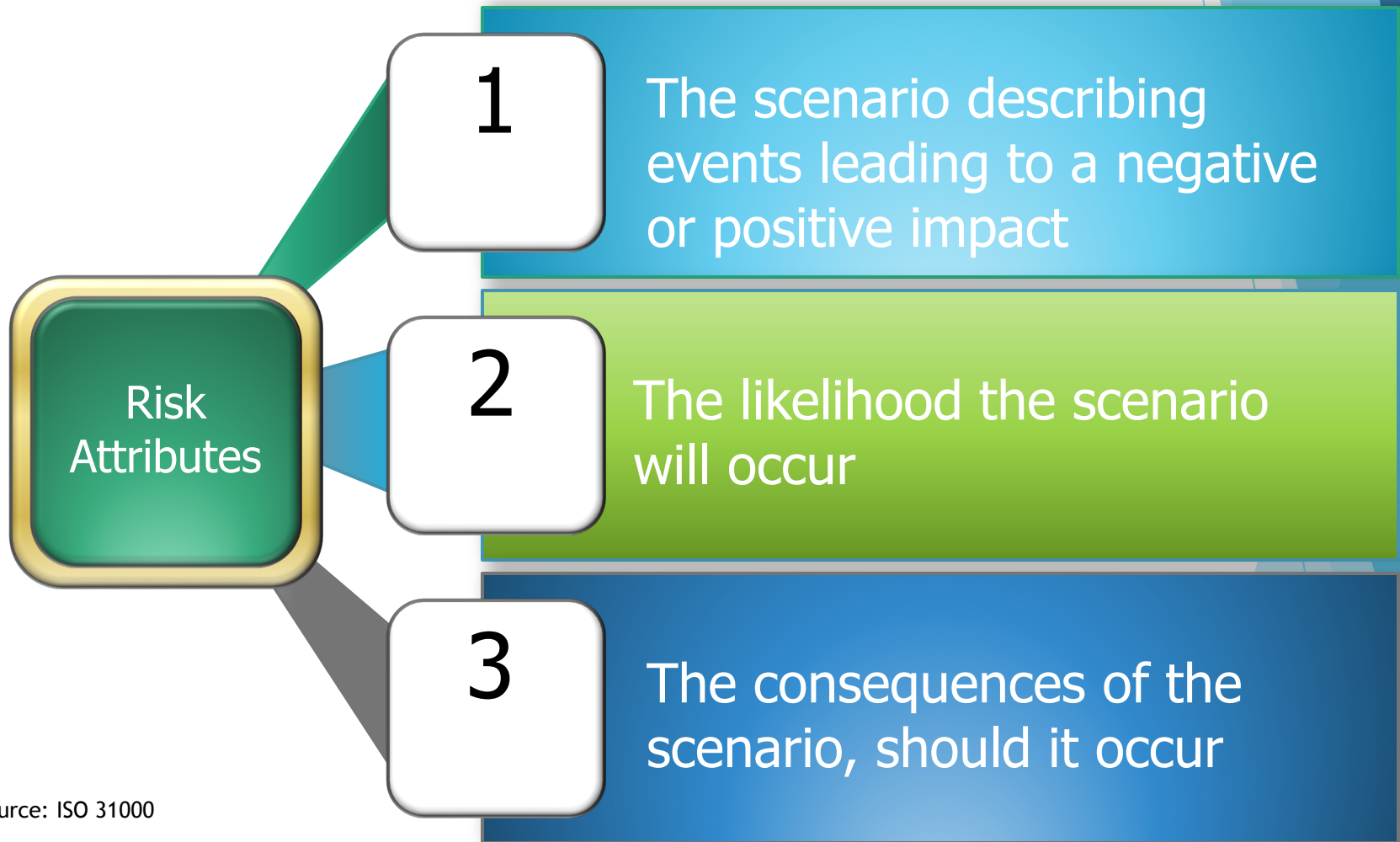


What is Enterprise Risk Management?



“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.”





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.

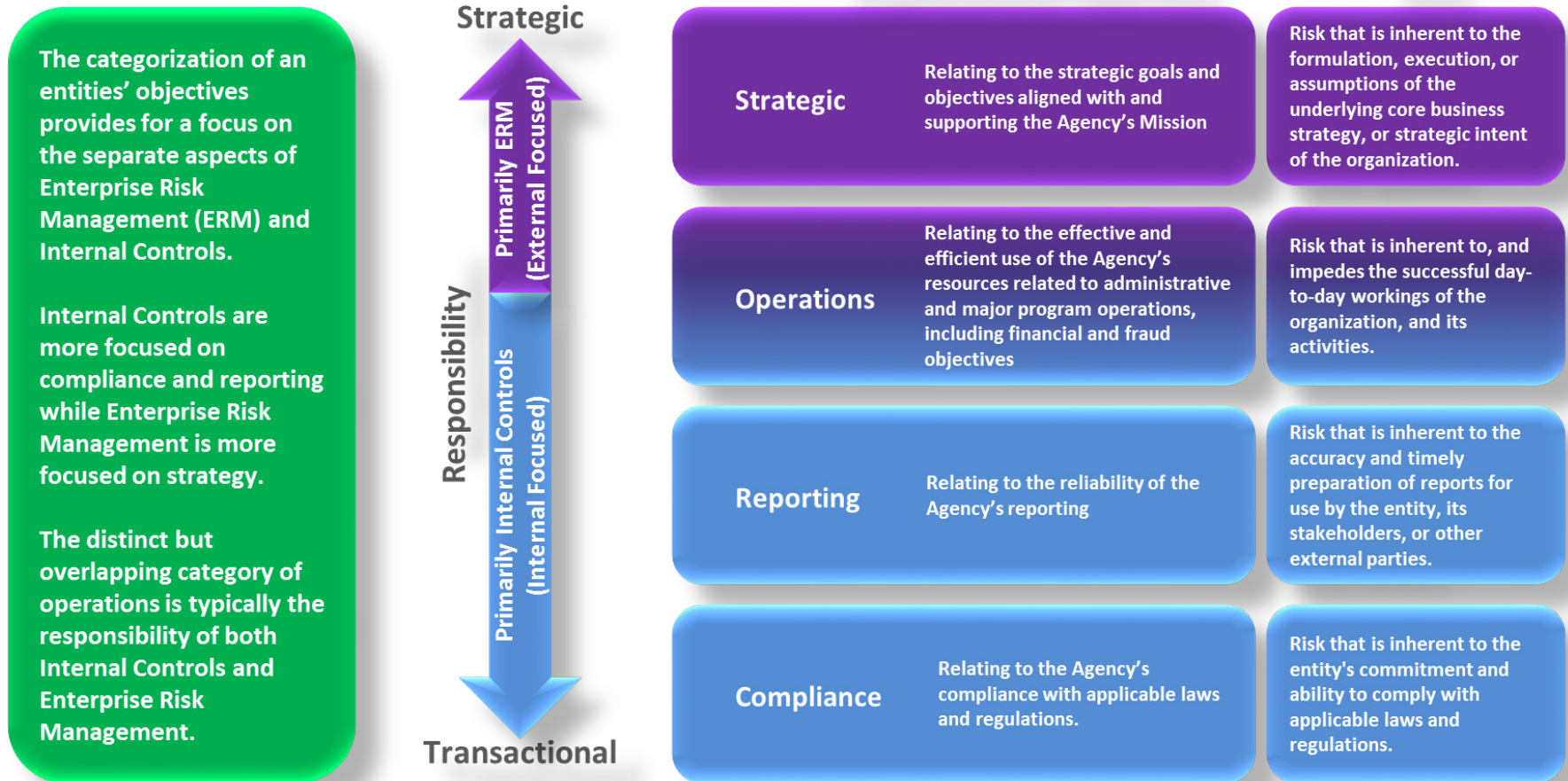
OMB View of A-123 (Internal Controls) and Enterprise Risk Management (ERM)



A-123 ERM Implementation Requirements



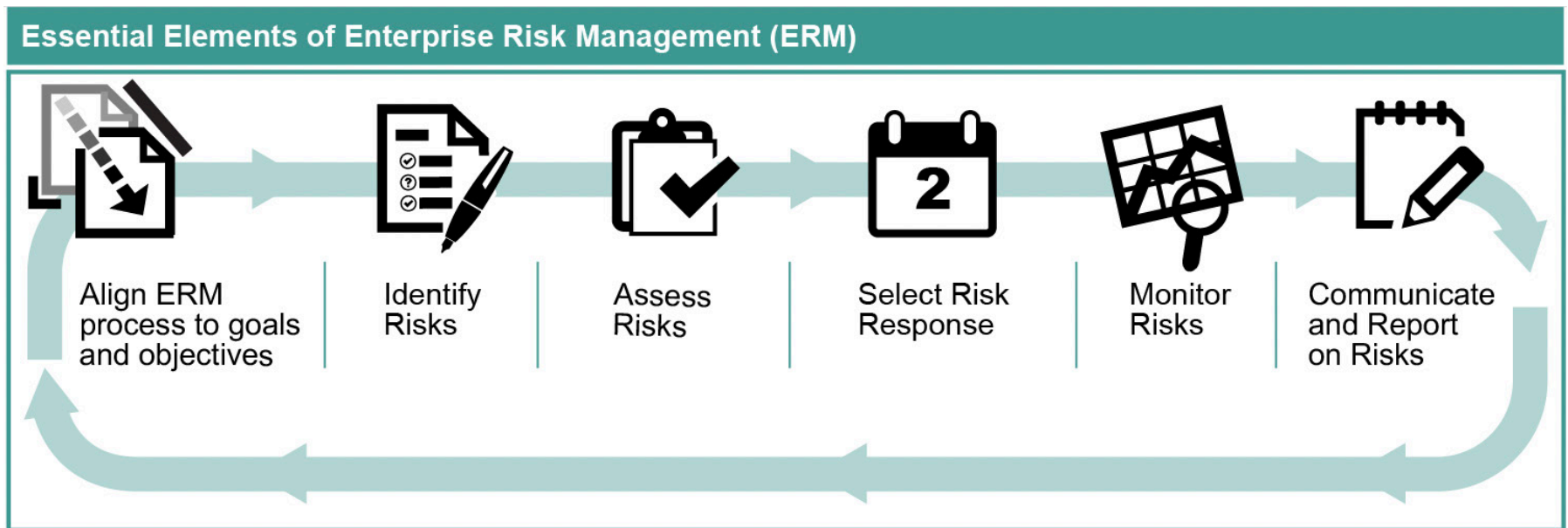
Portfolio View of the Relationship Between Strategy, Organizational Objectives, and Risks



Target Operating Model - ERM Integration

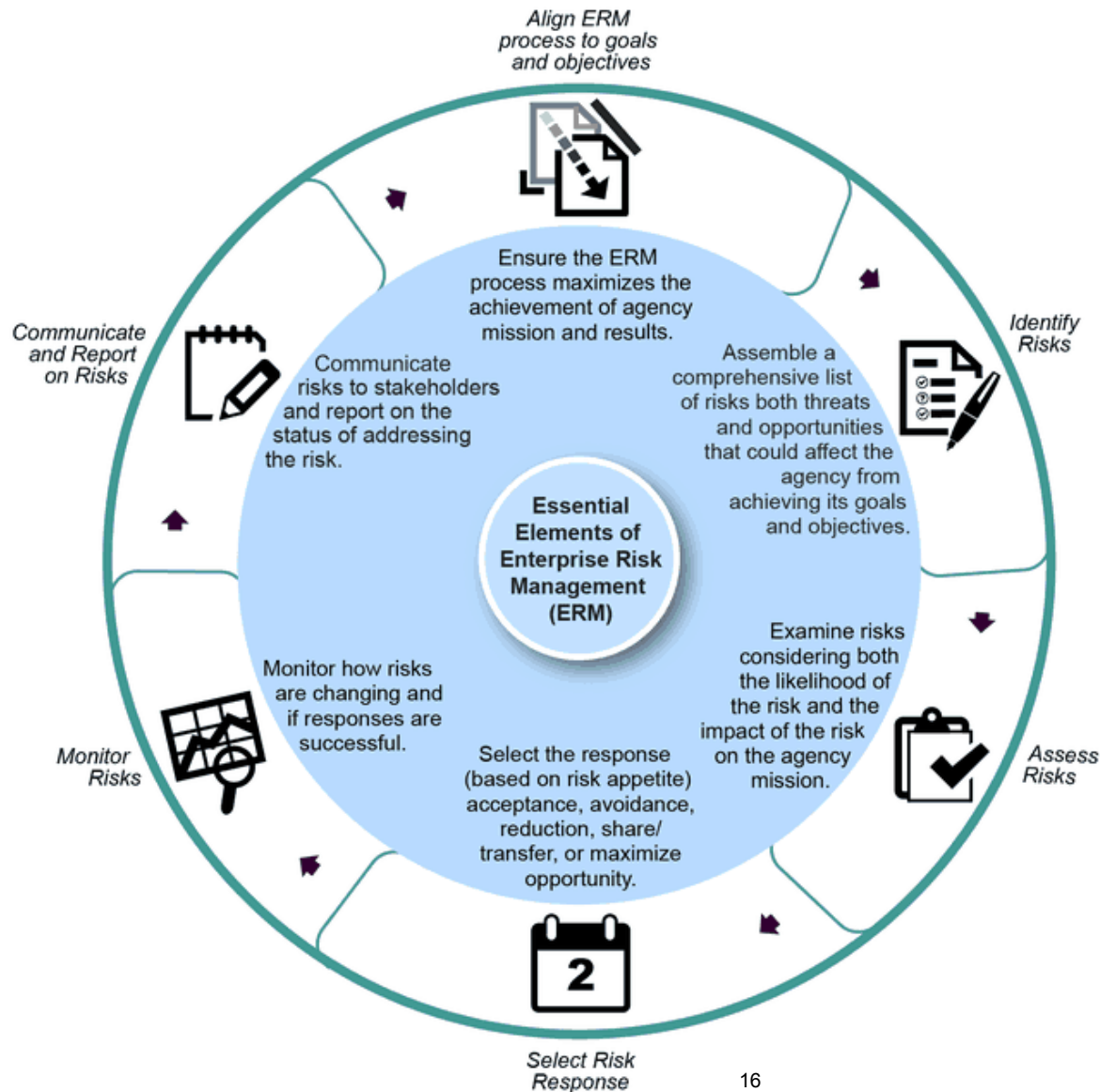
Strategy	Performance	Budget	Capital
<ul style="list-style-type: none">• Objective alignment• Risk Appetite & Tolerance informs mission priorities• Root cause identification• Enterprise view of common risk, objectives and potential mitigation strategies• Opportunities to collaborate	<ul style="list-style-type: none">• Measurement and monitoring of progress against goals and Risk Appetite & Tolerance• Risk monitoring of mitigation strategies and investments to validate effectiveness• KRIs monitor emerging risks• Risk forecasting and stress testing• Budget	<ul style="list-style-type: none">• Investments are driven by strategic investment criteria and risk mitigation strategies• Integrated governance structure drives decisions• Performance objectives defined	<ul style="list-style-type: none">• Strategic Initiatives Identified• Integrated governance structure drives decisions• Investment criteria, KPIs and KRIs inform decisions made in this process• Includes human, IT, and infrastructure investment prioritization

Essential Elements of ERM (GAO)



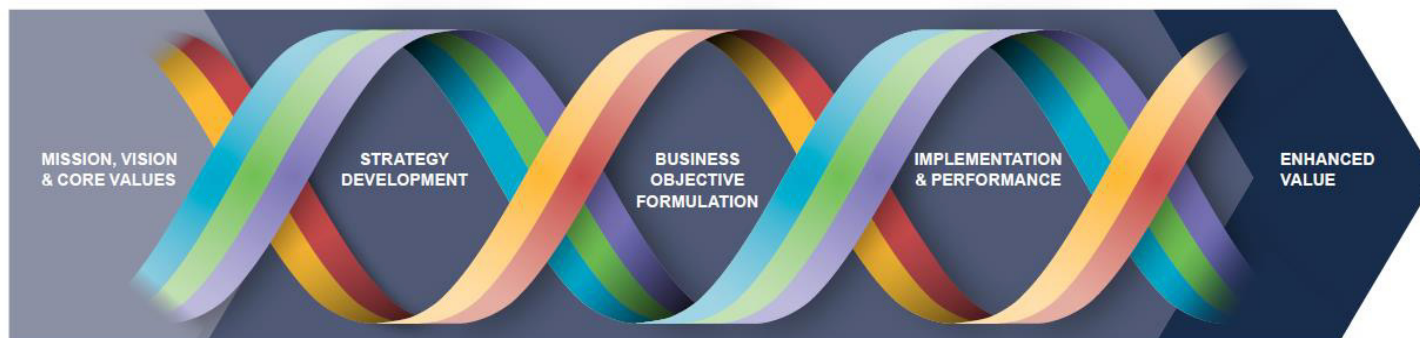
Source: GAO. | GAO-17-63

Essential Elements of ERM (GAO)



COSO ERM FRAMEWORK AND KEY Principles

ENTERPRISE RISK MANAGEMENT



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

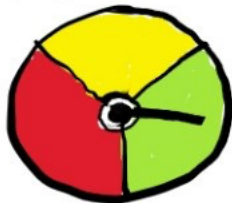
Figure 1. Evolving risk landscape 2008-2018

	2008	2013	2018
Top 5 Global Risks in terms of likelihood	Asset price collapse	Severe income disparity	Extreme weather events
	Middle East instability	Chronic fiscal imbalances	Natural disasters
	Failed and failing states	Rising greenhouse gas emissions	Cyberattacks
	Oil and gas price spike	Water supply crises	Data fraud or theft
	Chronic disease, developed world	Mismanagement of population ageing	Failure of climate-change mitigation and adaptation
Top 5 Global Risks in terms of impact	Asset price collapse	Major systemic financial failure	Weapons of mass destruction
	Retrenchment from globalization (developed)	Water supply crises	Extreme weather events
	Slowing Chinese economy (<6%)	Chronic fiscal imbalances	Natural disasters
	Oil and gas price spike	Diffusion of weapons of mass destruction	Failure of climate-change mitigation and adaptation
	Pandemics	Failure of climate-change mitigation and adaptation	Water crises

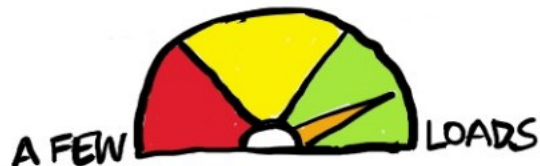
Committee of Sponsoring Organizations of the Treadway Commission(COSO)
and the World Business Council for Sustainable Development (WBCSD).
Preliminary Draft, January 2018

RISK GOVERNANCE DASHBOARD

NUMBER OF MEETINGS



NUMBER OF RISKS IDENTIFIED



WEIGHT OF RISK REPORTS



AUDIT OVERKILL



WELL,
THAT'S ALL
RIGHT THEN





Next Presentation



Enterprise Risk Management – Briefing for Federal Accounting Standards Advisory Board

February 2018



Enterprise Risk Management

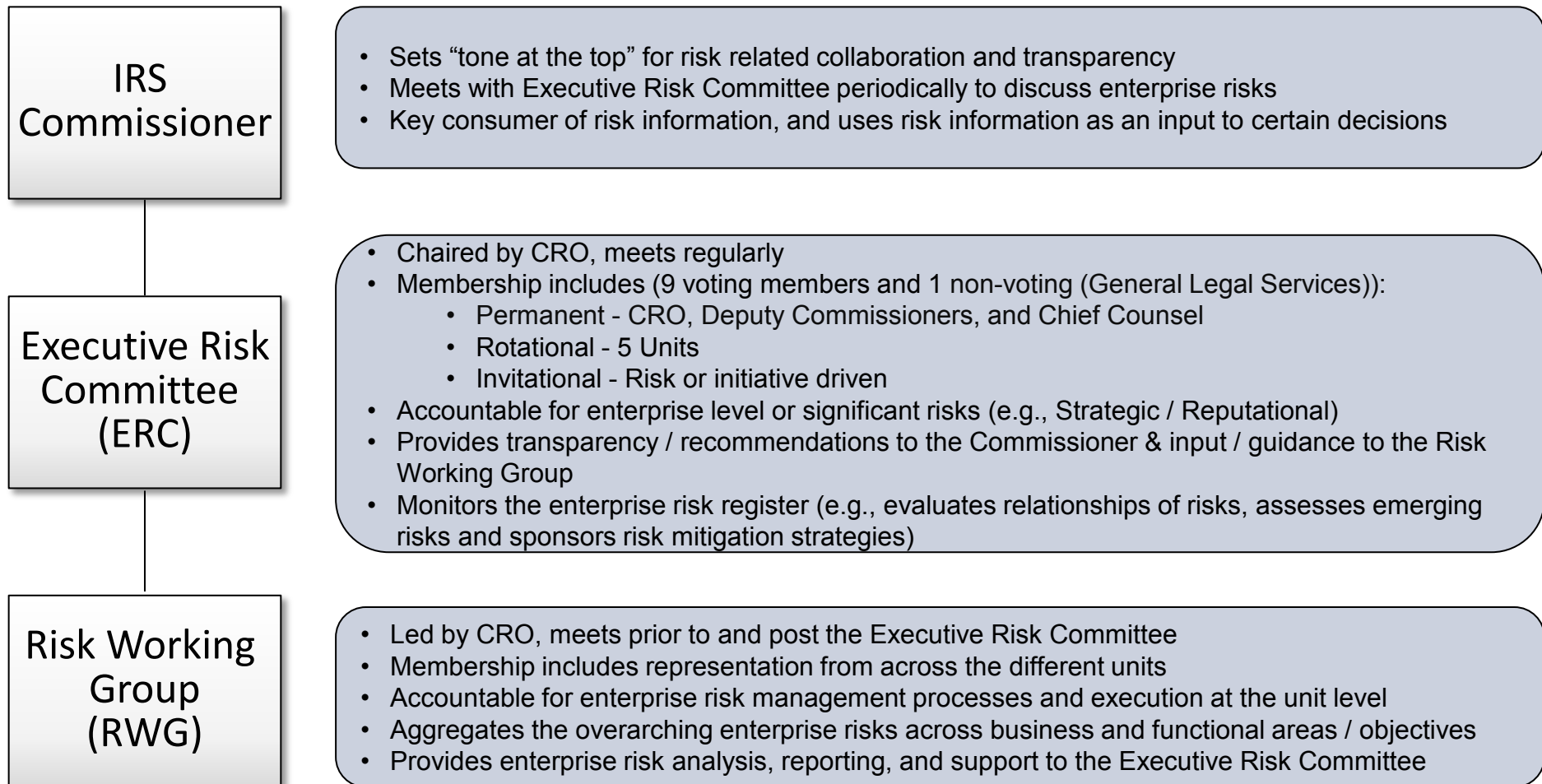
Chief Risk Officer (CRO)

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.



Purpose of Risk Assessments

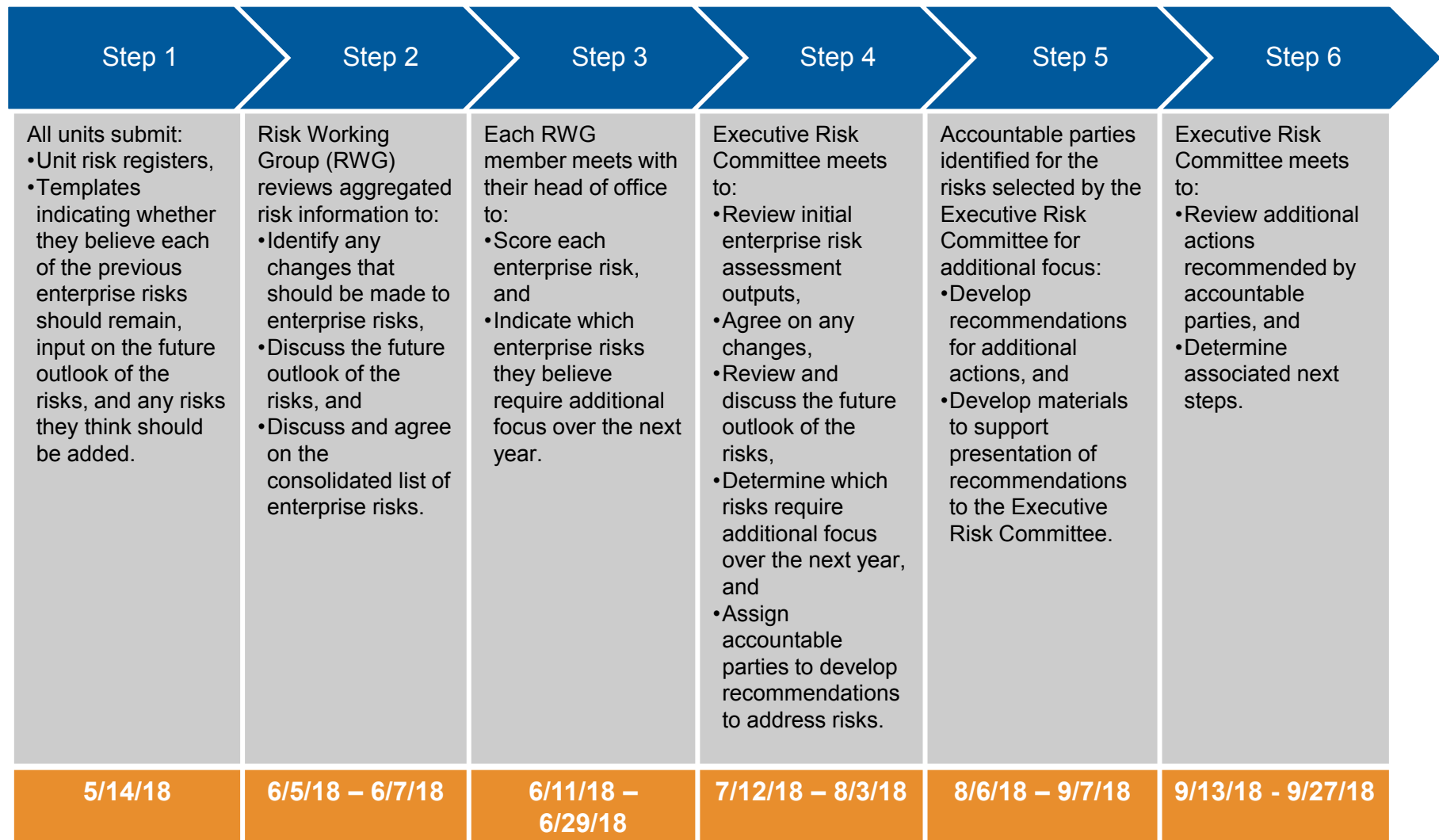
The purpose of risk assessments is to provide management an opportunity to:

- 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



IRS Risk Assessment Process

Enterprise Risk Assessment Process

Objectives

Key Inputs

Business Unit Risk
Information Set

Oversight / Audit Risk
and Issue Information
Set

Self Assessments

Interviews / Focus
Groups

Identify
Inherent
Risk

Identify
Mitigants

Assess
Residual
Risk

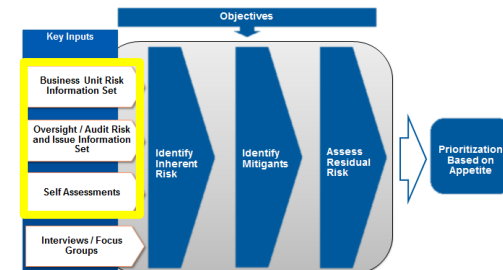
Prioritization
Based on
Appetite

Risk Types and Categories

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.

Risk Type	Definition	Risk Categories	
Strategic / Reputational	Aligned with and directly related to the IRS mission	<ul style="list-style-type: none"> • Mission/Scope • Trust, Confidence and Reputation 	<ul style="list-style-type: none"> • Customer Service • Enforcement
Financial / Reporting	Reliability of the overall financial well-being of the IRS and the U.S. tax system	<ul style="list-style-type: none"> • Budget • Tax Fraud • Administrative Fraud • Improper Payments 	<ul style="list-style-type: none"> • Tax Complexity • Stewardship of Taxpayer Dollars • External Reporting
Legal / Regulatory	IRS compliance with applicable laws and regulations	<ul style="list-style-type: none"> • Laws & Regulations • Litigation 	<ul style="list-style-type: none"> • Taxpayer Rights & Protection
Operational	Effectiveness and efficiency of the IRS's operations	<ul style="list-style-type: none"> • Program/Operational Effectiveness • Information/Data Reliability & Sufficiency 	<ul style="list-style-type: none"> • Management Oversight • Disruption to Operations • Physical Security
Organizational	Effectiveness of the IRS's structure, culture, and people	<ul style="list-style-type: none"> • Human Capital • Organizational Culture • Morale 	<ul style="list-style-type: none"> • Organizational Structure • Leadership
Technology	Effectiveness, efficiency and security of the IRS's technology	<ul style="list-style-type: none"> • Infrastructure • Information Security 	<ul style="list-style-type: none"> • Technical Effectiveness/Agility

IRS Risk Assessment Process



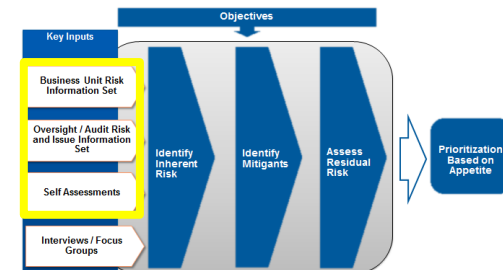
Identifying Changes to Key Internal and External Factors and Considering Impact on Risk Profile

- 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:

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

- 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.

IRS Risk Assessment Process



Identifying Changes to Key Internal and External Factors and Considering Impact on Risk Profile (Contd.)

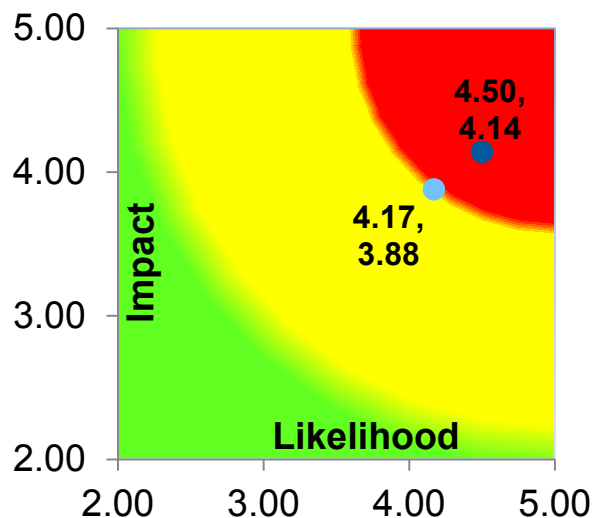
- Consider factors in the internal environment across each of the following categories:

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

- 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.

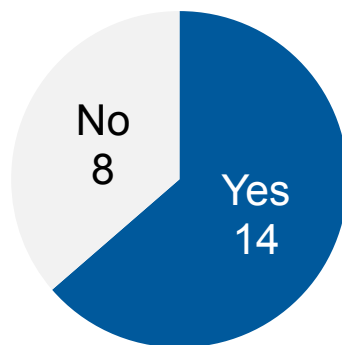
2017 Enterprise Risk Summary – SAMPLE RISK OVERVIEW

Primary Strategic Goal Impacted	4. Cultivate a well-equipped, diverse, flexible, and engaged workforce																				
Enterprise Risk	#	Name							Description												
	3	Critical Staffing Shortages							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.												
Relationships with other Enterprise Risks	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Total
	X	X					X				X							X			5
																					# of Unit Risks Mapped
																					46

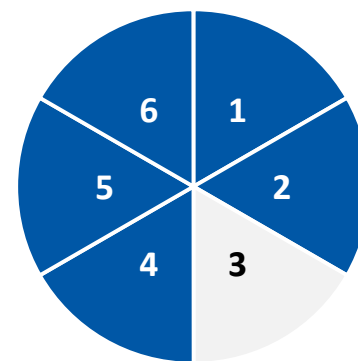


● 2016 Score ● 2017 Score

of Units that Said this Risk Requires Add'l Focus



Strategic Goals



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

Outcomes of Enterprise Risk Assessments

Year	Outputs	Outcomes
2014	<ul style="list-style-type: none"> • 15 enterprise risks • Likelihood and impact scores 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 29 enterprise risks • 6 top enterprise areas of risk • Assigned accountable parties for actions for each of 6 top enterprise areas of risk 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 22 enterprise risks • Likelihood and impact scores • 5 top enterprise risks • Assigned accountable parties for the top five enterprise risks 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 20 enterprise risks • Likelihood and impact scores • 5 top enterprise risks • Assigned accountable parties for all enterprise risks 	<ul style="list-style-type: none"> • 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.

IRS ERM Progress and Continued Growth

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

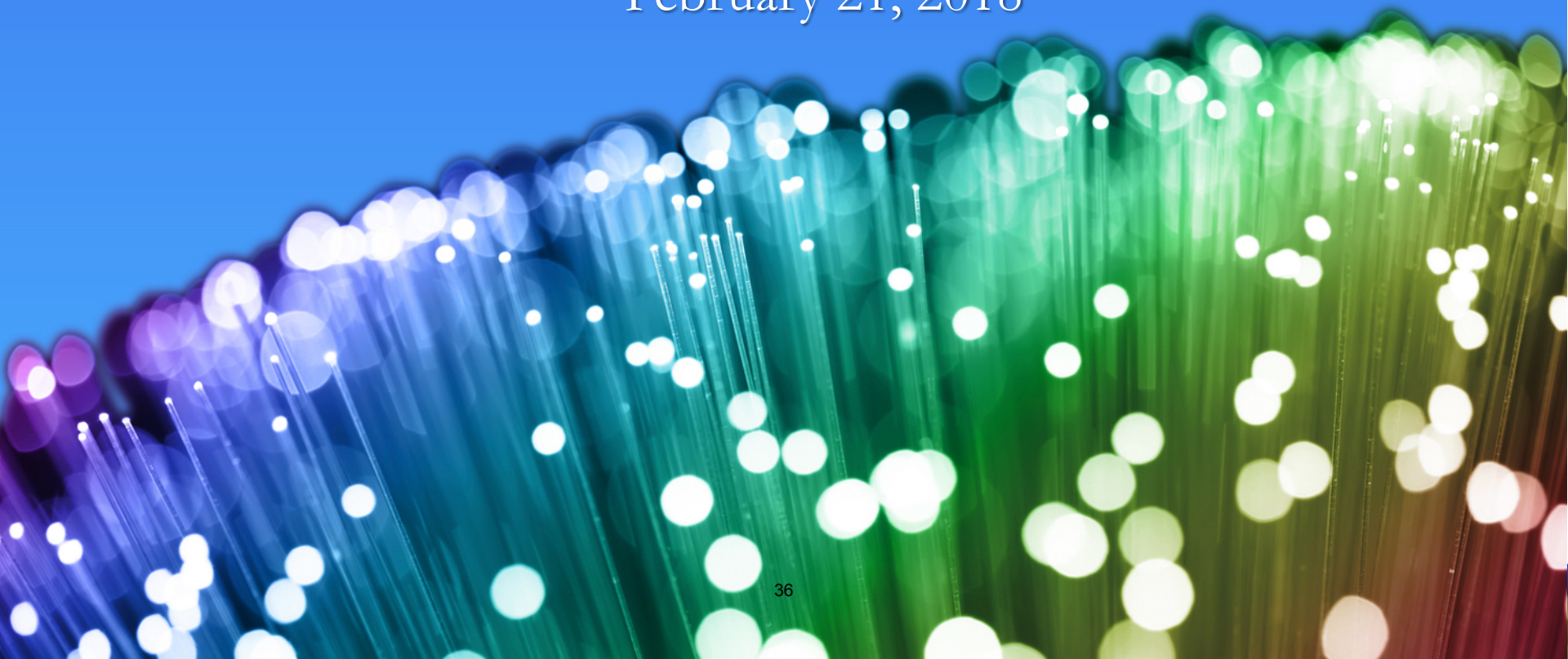


Enterprise Risk Management Risk Profiling

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.”

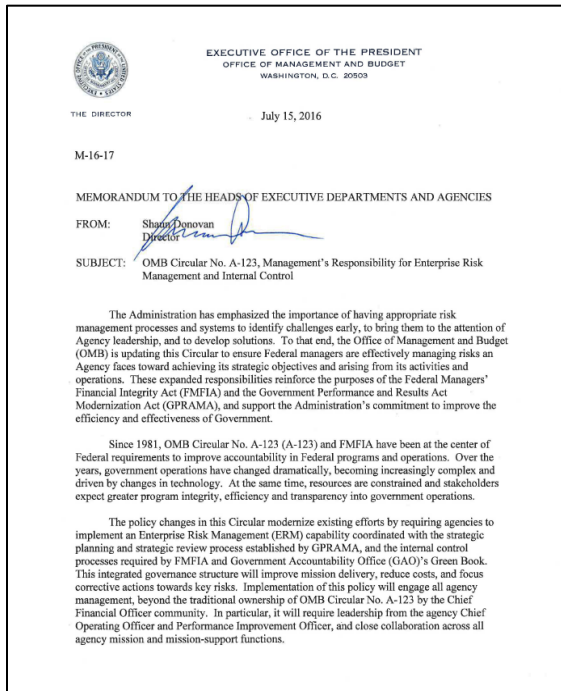
This briefing will attempt to meet FASAB’s objective by covering:

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.
- Its 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

Risk appetite is important here

STRATEGIC OBJECTIVE – Improve Program Outcomes								
Risk	Inherent Assessment		Current Risk Response	Residual Assessment		Proposed Risk Response	Owner	Proposed Risk Response Category
	Impact	Likelihood		Impact	Likelihood			
Agency X may fail to achieve program targets due to lack of capacity at program partners.	High	High	REDUCTION: Agency X has developed a program to provide program partners technical assistance	High	Medium	Agency X will monitor capacity of program partners through quarterly reporting from partners	Primary – Program Office	Primary – Strategic Review
OPERATIONS OBJECTIVE – Manage This Risk of Fraud in Federal Operations								
Contract and Grant fraud.	High	Medium	REDUCTION: Agency X has developed procedures to ensure contract performance is monitored and that proper checks and balances are in place.	High	Medium	Agency X will provide training on fraud awareness, identification, prevention, and reporting.	Primary – Contracting or Grants Officer	Primary – Internal Control Assessment

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



Illustrative DHS Example

Department of Homeland Security FY 2017 Agency Financial Report



*With honor and integrity, we will safeguard the
American people, our homeland, and our values.*



 [We are DHS](#)

“DHS manages risk ever 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.”



Source: https://www.dhs.gov/sites/default/files/publications/dhs_agency_financial_report_fy2017_1.pdf

Illustrative NSF Example



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

Source: <https://www.nsf.gov/pubs/2018/nsf18020/pdf/nsf18020.pdf>



COSO Framework and Risk Appetite Principle

COSO's Enterprise Risk Management Framework - June 2017

ENTERPRISE RISK MANAGEMENT



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

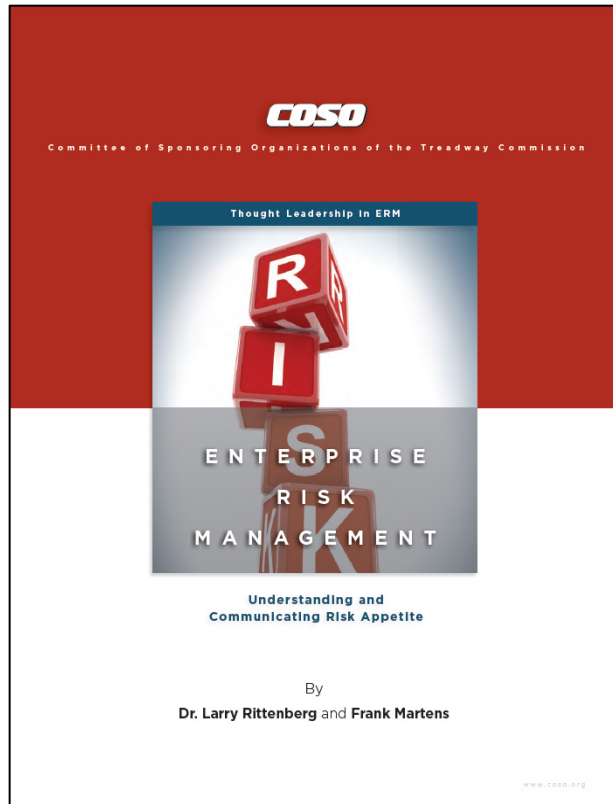
Risk Appetite

- 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.....



- Oldie but Goodie whitepaper:
<https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf>
- 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



Definition of Risk

- 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.*



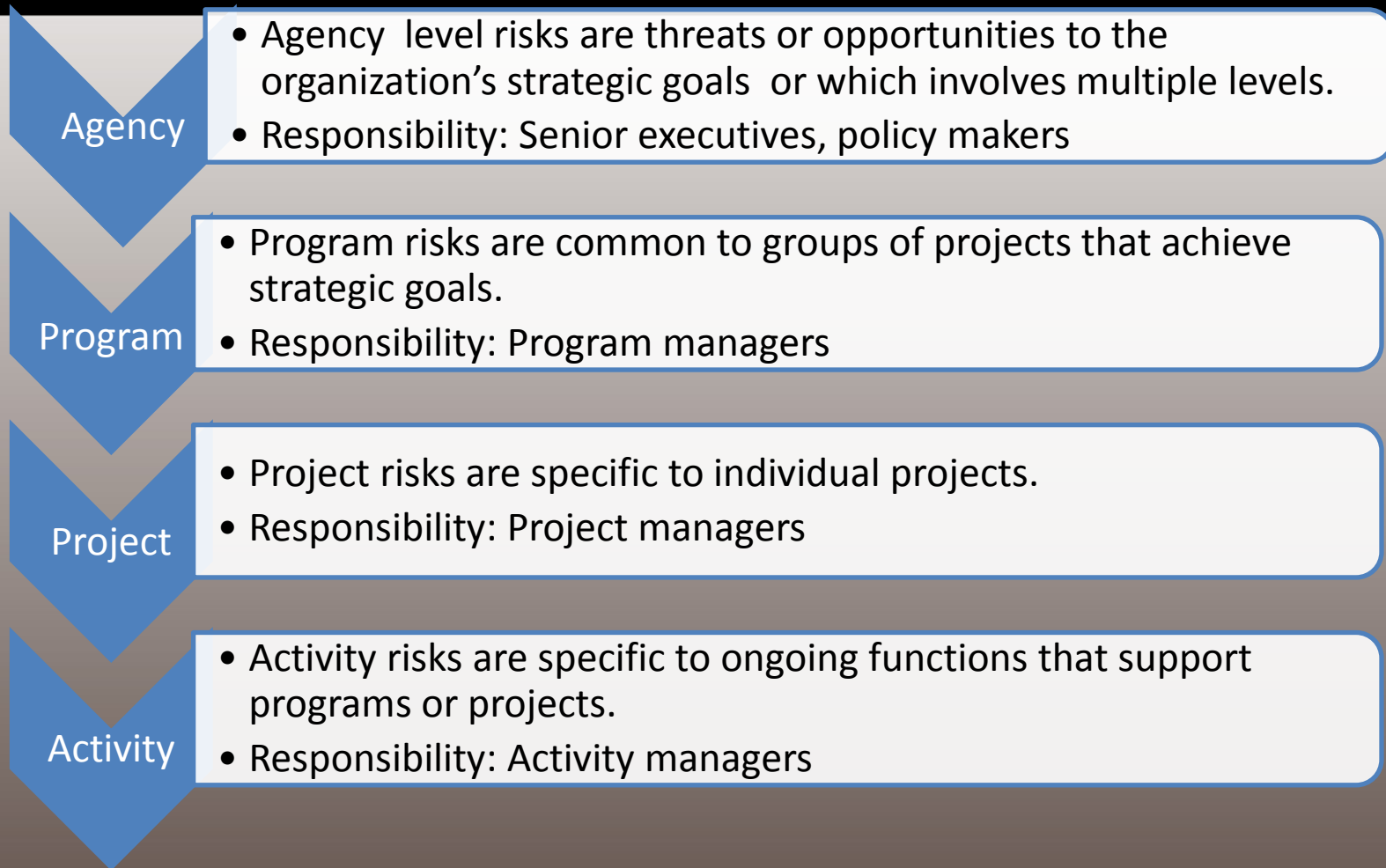
FHWA Mission, Vision, Values

- 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.

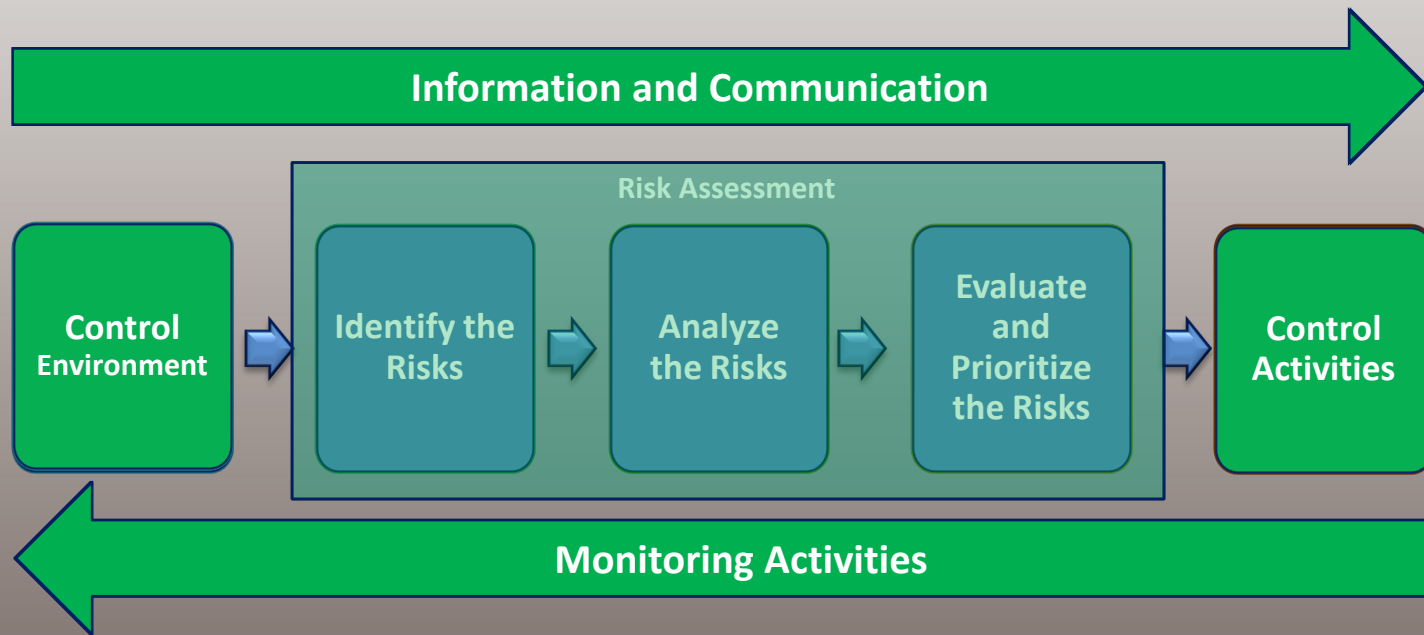


Who Manages Risk?

Consider risk at different levels of the organization



Risk Management Process and Components of Internal Control



Updated for 2016

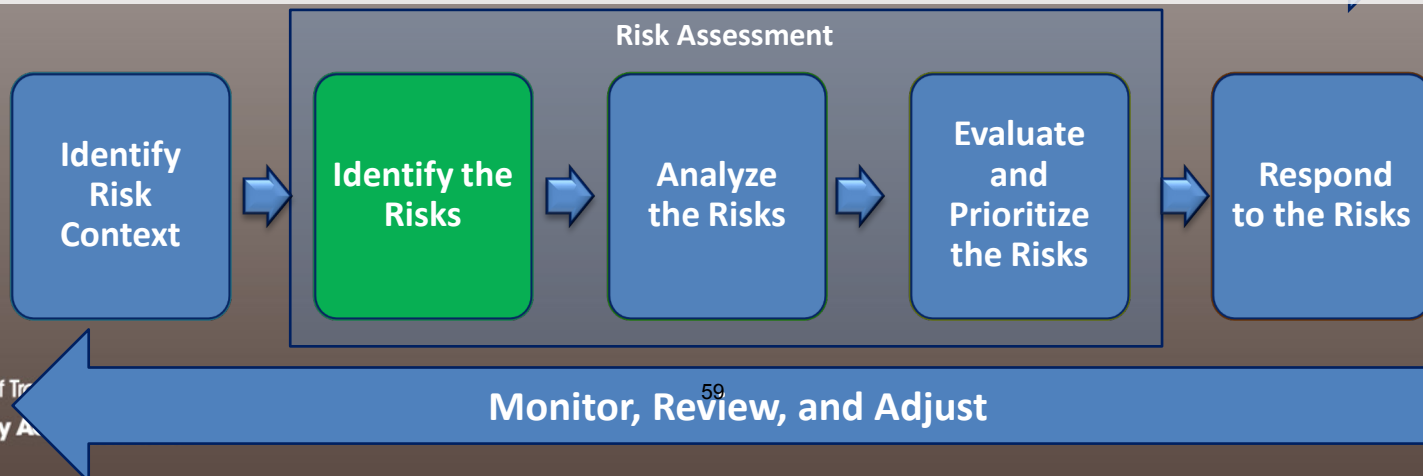


		Risk Management Process Step	Key Questions
		Communication and Consultation	Who needs to be involved? How will we communicate and consult with them?
		Identify the Context	What program or other objective areas will we assess? What are the things to consider when we assess them? <i>What are the existing controls and how are they working? How do you know?</i> What criteria will we use to assess our risks? Who will do the assessment?
Risk Assessment		Identify the Risks	What events could happen that would affect my objectives? What are the corresponding impacts? What are my If...then... statements?
		Analyze– Assess Impact	What is the severity of this impact according to my criteria?
		Analyze– Assess Likelihood	What is the likelihood that this risk event will occur?
		Prioritize Risks	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?
		Plan and Execute Risk Response Strategies	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?
		Monitor, evaluate, and adjust	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?



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.



Risk Short Description	Event	Impact
Impacts from delayed funding	If funding (CR's, re-statements, transfers) and notifications (Form FHWA-370 and advices) are not received in a timely manner.	Then new projects may not be started and current projects could be delayed; funding opportunities could be lost; payroll processing may be delayed.
Performance Management	If the Notice of Proposed Rulemaking does not get issued as scheduled	then State DOTs and MPOs will not be able to comply with the law.
Innovation	If we fail to implement a coordinated Infrastructure research program to identify, promote and implement innovation	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
10-yr PE	If the state does not adhere to 23 CFR 630.112(c)(2), (10-year PE requirements)	then the state may/will be required to pay back significant amount of money.
Utility-Investigation (Design)	If adequate utility investigation is not performed during design.	Then conflicts will continue to arise during construction which may increase cost and contract time.
System Changes	If the FMIS modernization implementation, Current Bill System, or E-Travel are delayed or encounter significant issues,	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.
FMIS 5.0 Implementation	If obstacles are encountered during FMIS 5.0 implementation,	then project authorizations may be substantially delayed and project data quality may be inconsistent.
Billing Risks with FMIS 5.0 and IRIS	If there are not sufficient billing controls in place with transition to FMIS 5.0 and IRIS,	then improper payments may be processed.
Planning through Construction Obligation	If the links between project planning and construction authorization are not improved,	then projects will continue to be programmed for construction without having completed project development, which leads to delays and increased project costs.
QA/QC Bonuses	If the State pays excessive amounts of QA/QC bonuses to contractors,	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.

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.



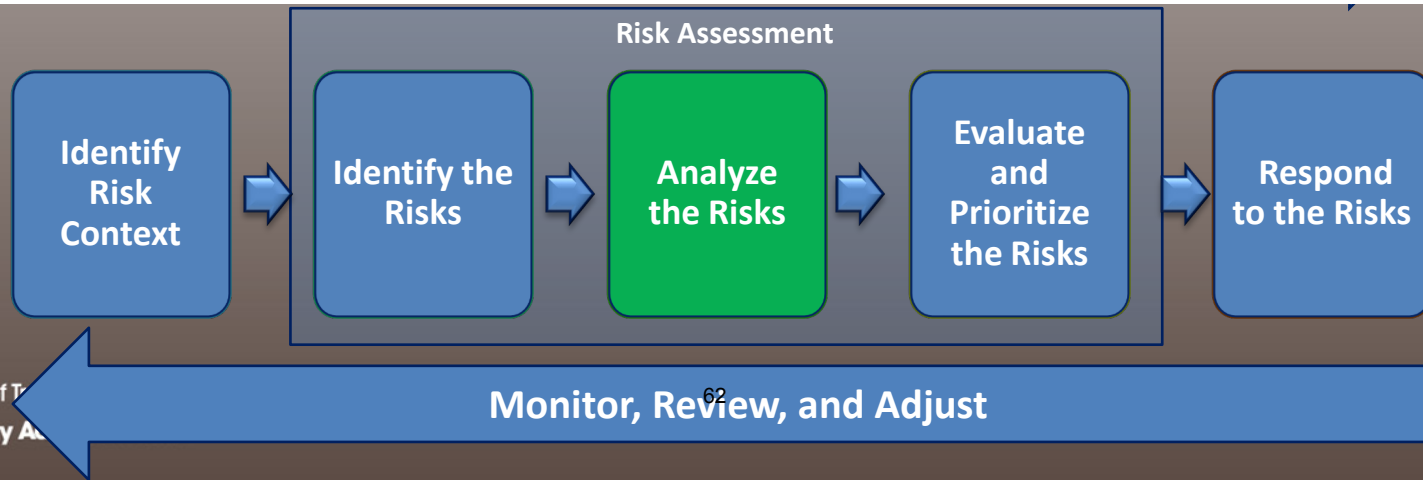
Impact Criteria

◆ Scale

- ◆ Catastrophic
- ◆ Major
- ◆ Moderate
- ◆ Minor
- ◆ Insignificant

◆ Criteria

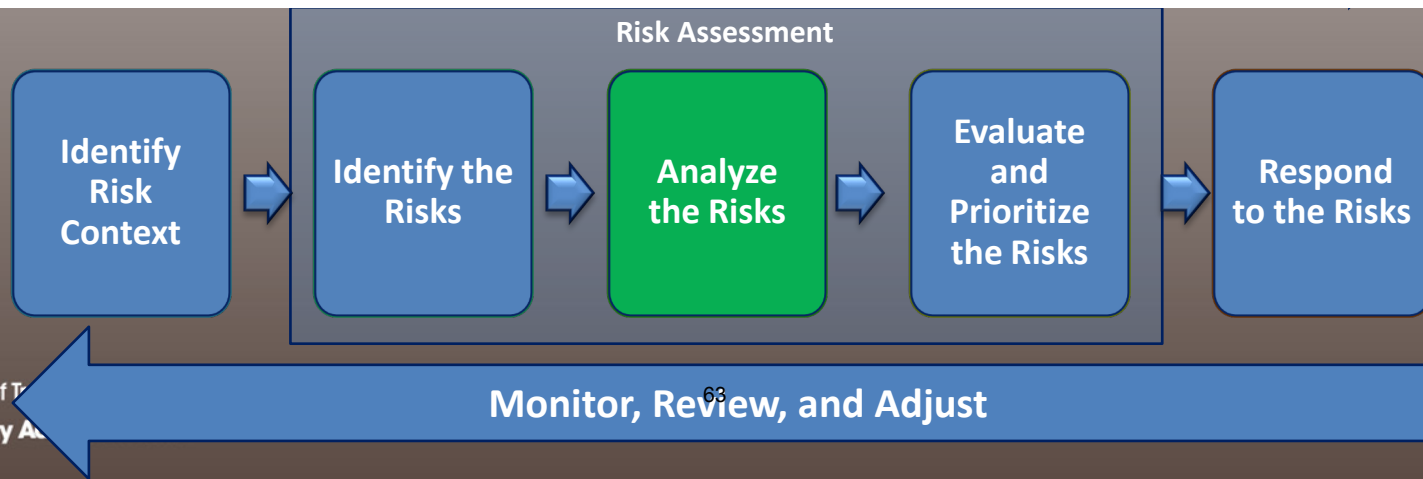
- Financial
- Reputation
- Business Operations
- Legal and Compliance
- Infrastructure Assets
- Resources and Effort Required
- Human and Natural Environment
- Safety
- Civil Rights
- Economic



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



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



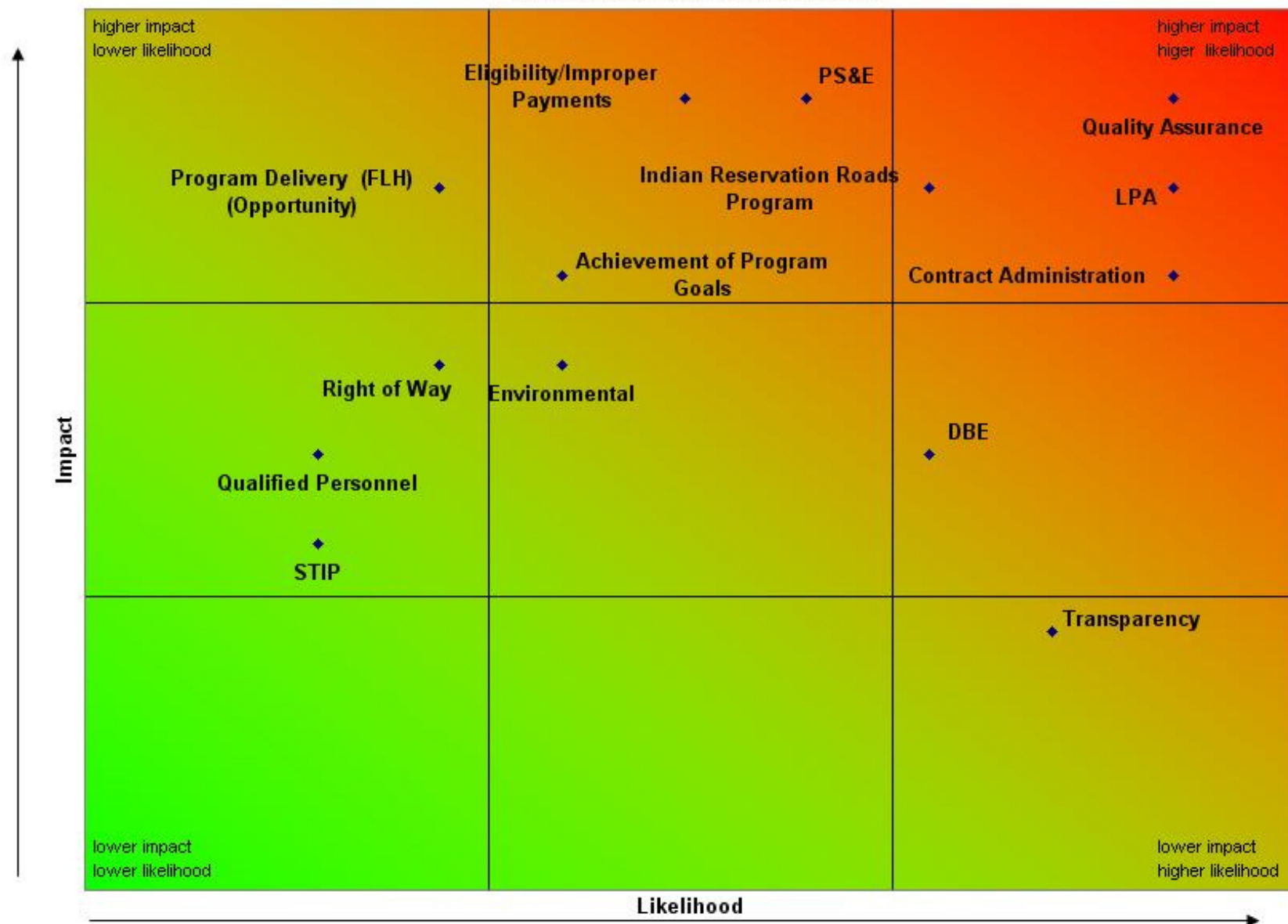
Heat Map Tool

- A graphical plot or visual tool used to represent the relative placement of risks. The expected value of the risk determines its location.



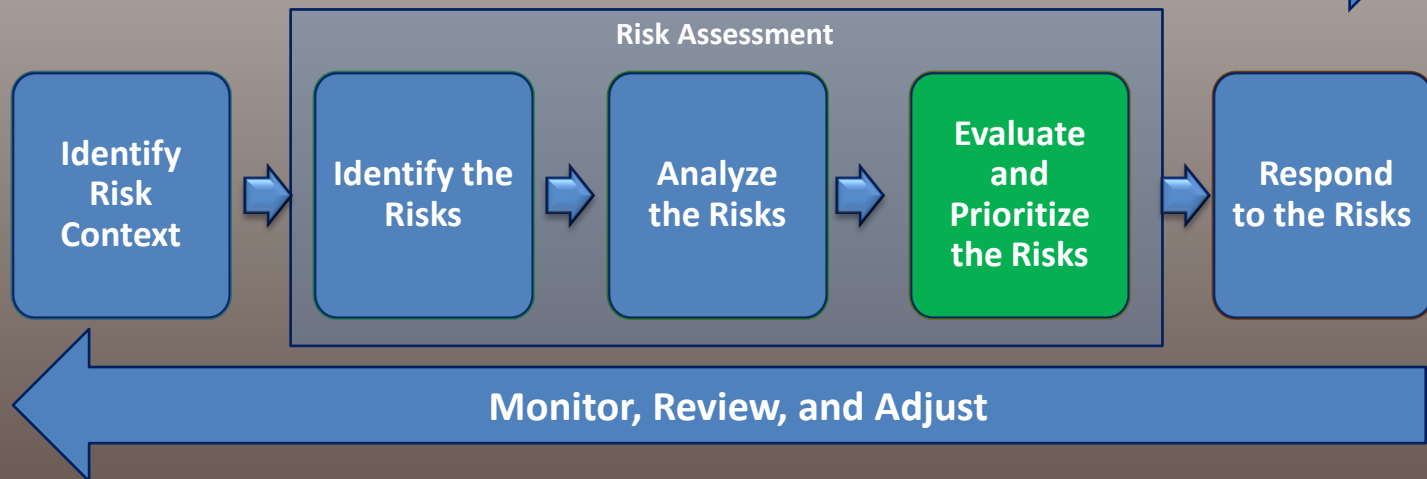
	Likelihood	Unlikely	Possible	Likely	Almost Certain
Impact	Description	The event could possibly occur, but is unlikely at this time.	The event could occur under specific conditions and some of those conditions are currently evidenced.	The event is most likely to occur in most circumstances.	The event is expected to occur in most circumstances or is happening now.
Catastrophic	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.				
Major	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.				
Moderate	Significant financial loss and variance to budget. Moderate embarrassment impacting short term effectiveness. Moderate operational impact, business not interrupted. Leads to reportable findings.				
Minor	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.				
Insignificant or Neutral	Minimal or no measurable operational impact. Can be managed with routine activities. Leads to immaterial audit findings.				

FHWA Recovery Act Risk Assessment



Leadership Validation

- 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

