

U.S. Department of Homeland Security
Office of Inspector General
Office of Enterprise Risk Identification & Management

Risk Informed Work Planning (Identifying the Unknown Unknowns at DHS)



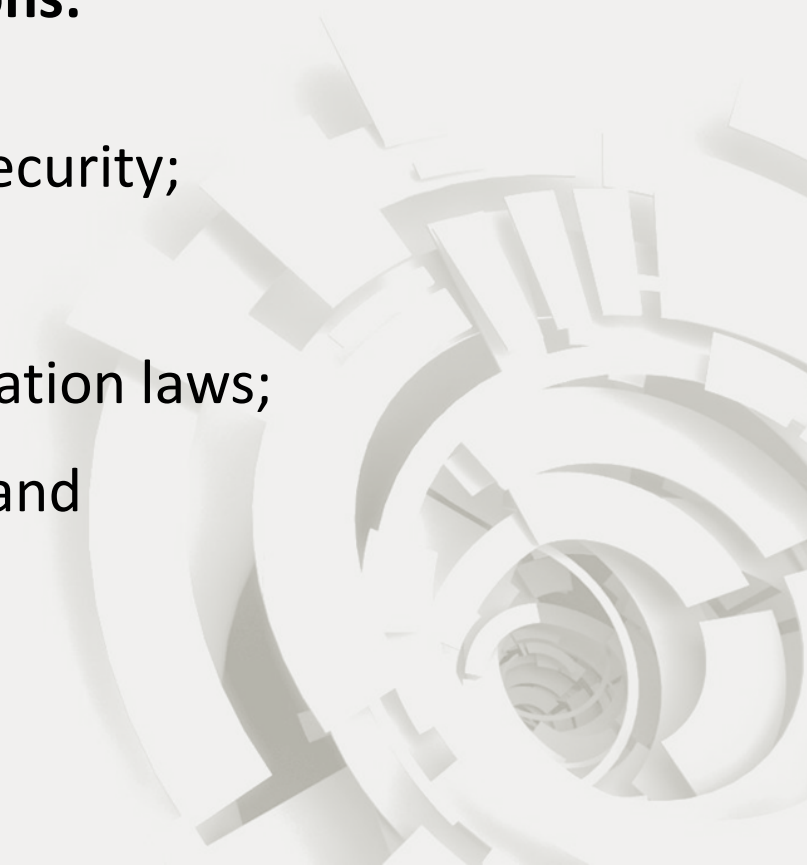
Learning Objectives

- Who we are
- What is risk?
- Why is it important to assess risk?
- How our office is driving risk informed work planning

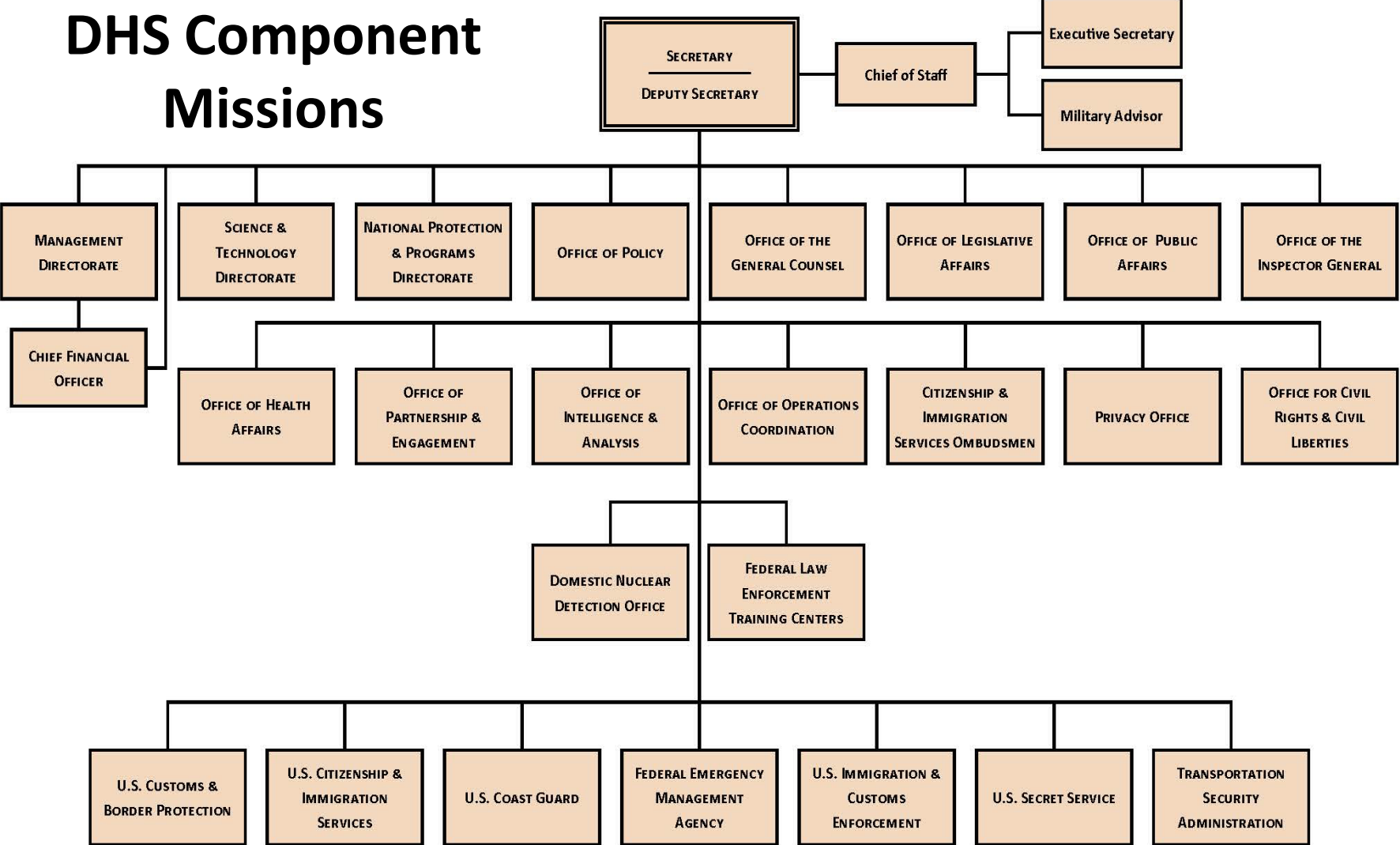


DHS' Mission

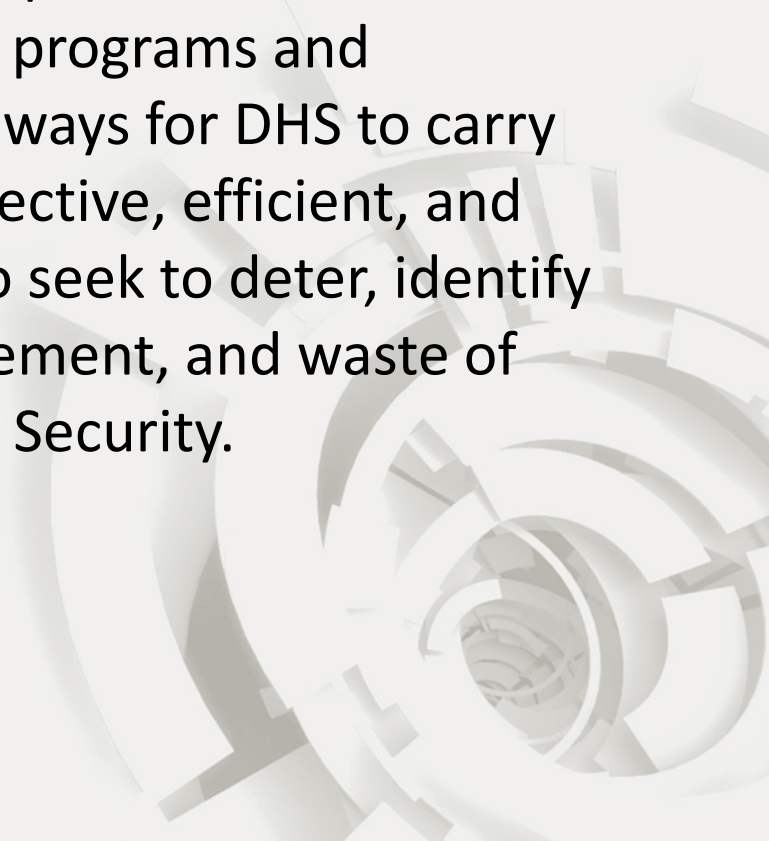
There are 5 homeland security missions:

1. Prevent terrorism and enhancing security;
 2. Secure and manage our borders;
 3. Enforce and administer our immigration laws;
 4. Safeguard and secure cyberspace; and
 5. Ensure resilience to disasters.
- 

DHS Component Missions



DHS-OIG's Mission

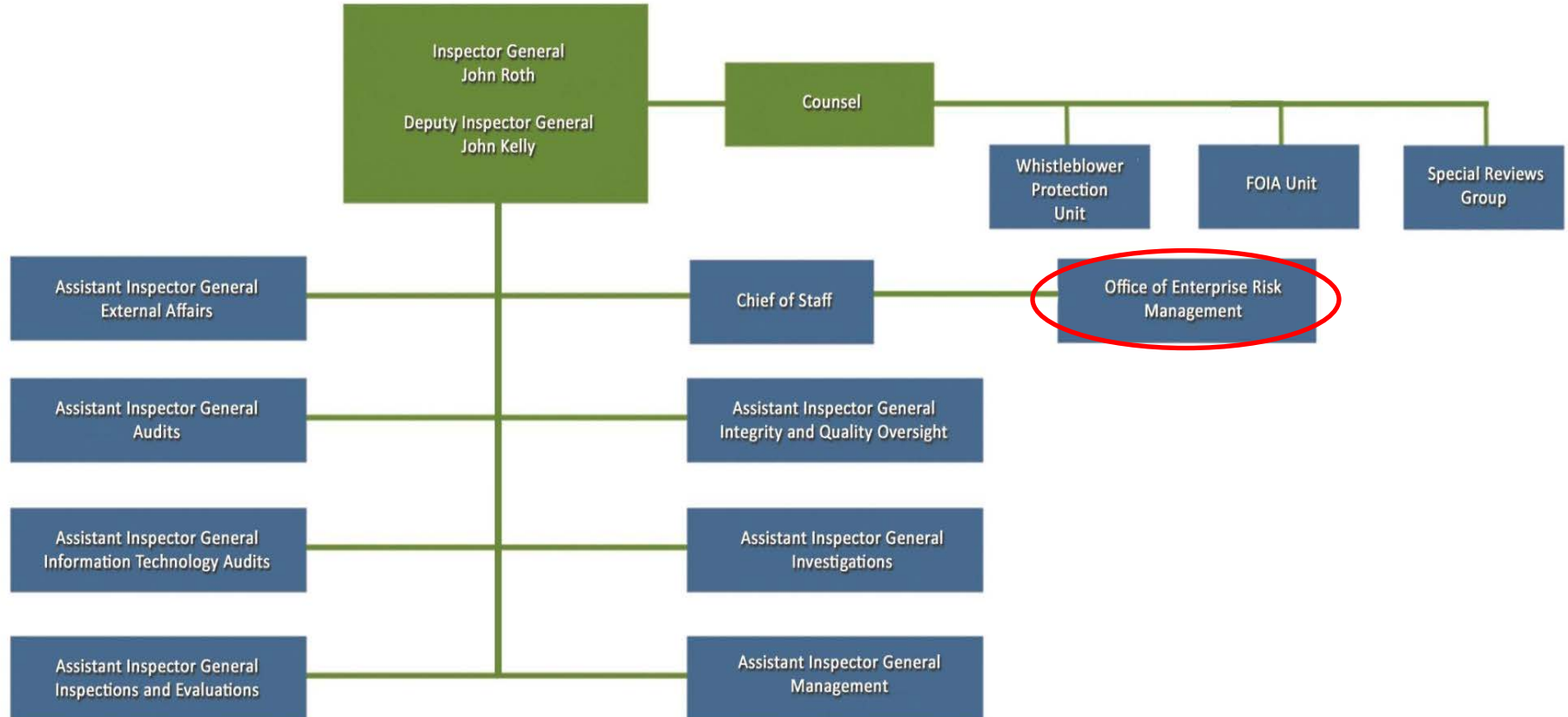
- The OIG conducts and supervises independent audits, investigations, and inspections of the programs and operations of DHS, and recommends ways for DHS to carry out its responsibilities in the most effective, efficient, and economical manner possible. We also seek to deter, identify and address fraud, abuse, mismanagement, and waste of taxpayer funds invested in Homeland Security.
- 

DHS-OIG's Mission

- Affect positive change...
 - In state & local programs and operations
 - In DHS program and operations
 - To prevent wasting taxpayer funds



Office of Enterprise Risk Identification & Management (OERIM)



What's a “risk”?

- What do you think of when someone mentions “risk”?



Different Perspectives of “risk”

- **Audit Risk:**

“**6.05** Audit risk is the possibility that the auditors’ findings, conclusions, recommendations, or assurance may be improper or incomplete, as a result of factors such as evidence that is not sufficient and/or appropriate, an inadequate audit process, or intentional omissions or misleading information due to misrepresentation or...Audit risk includes the risk that auditors will not detect a mistake, inconsistency, significant error, or fraud in the evidence supporting the audit.”

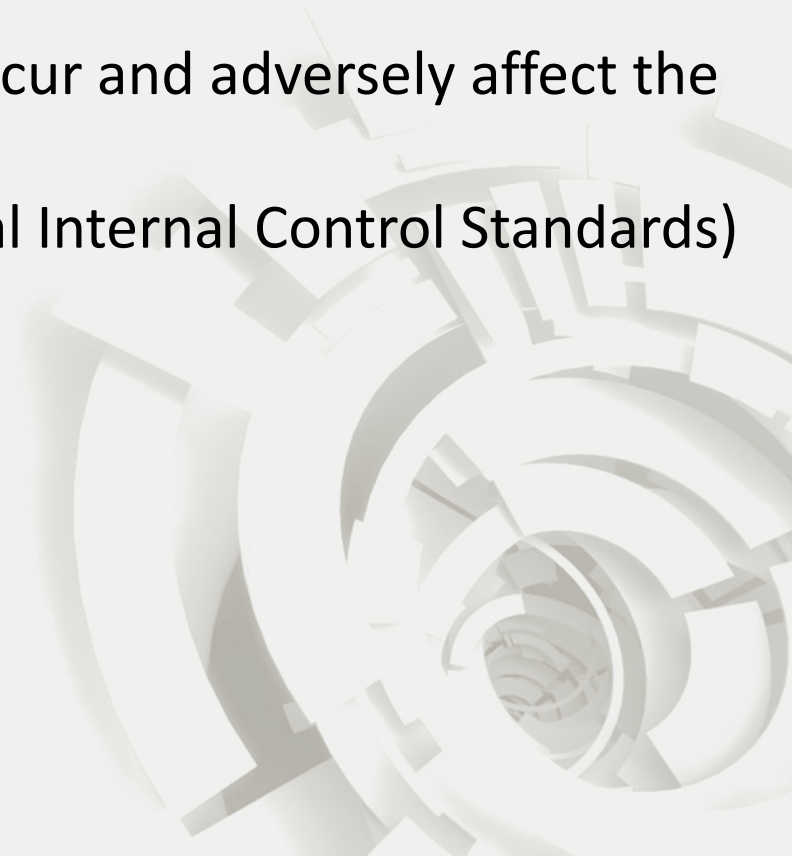
(Source: GAO-12-331G Government Auditing Standards)

Different Perspectives of “risk”

- **Risk:**

“The possibility that an event will occur and adversely affect the achievement of objectives.”

(Source: GAO-14-704G Federal Internal Control Standards)

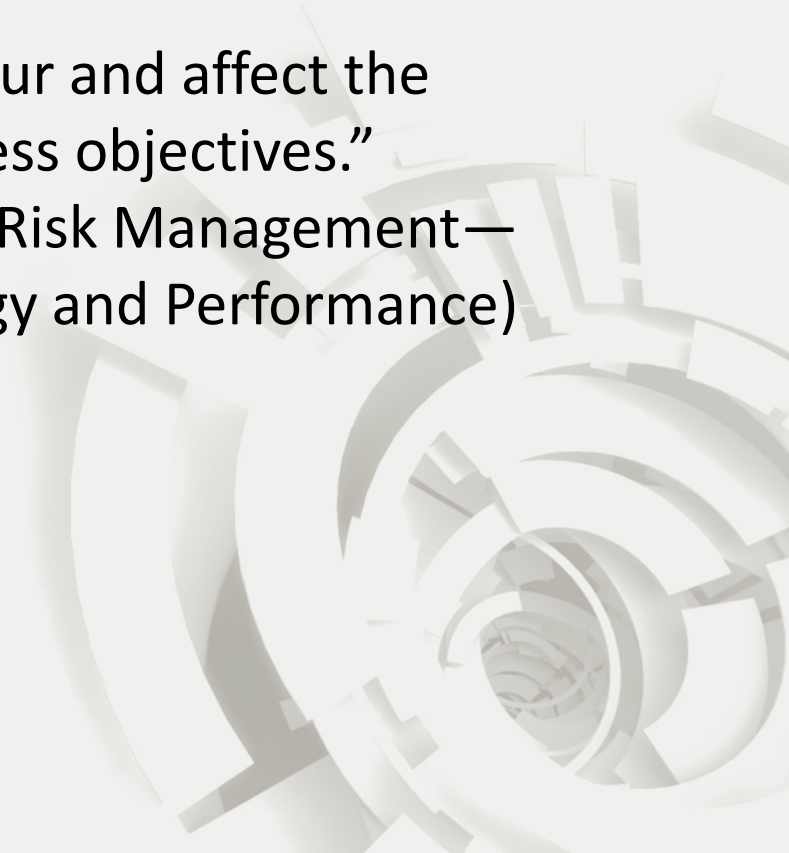


Different Perspectives of “risk”

- **Risk:**

“The possibility that events will occur and affect the achievement of strategy and business objectives.”

(Source: COSO Enterprise Risk Management—
Aligning Risk with Strategy and Performance)

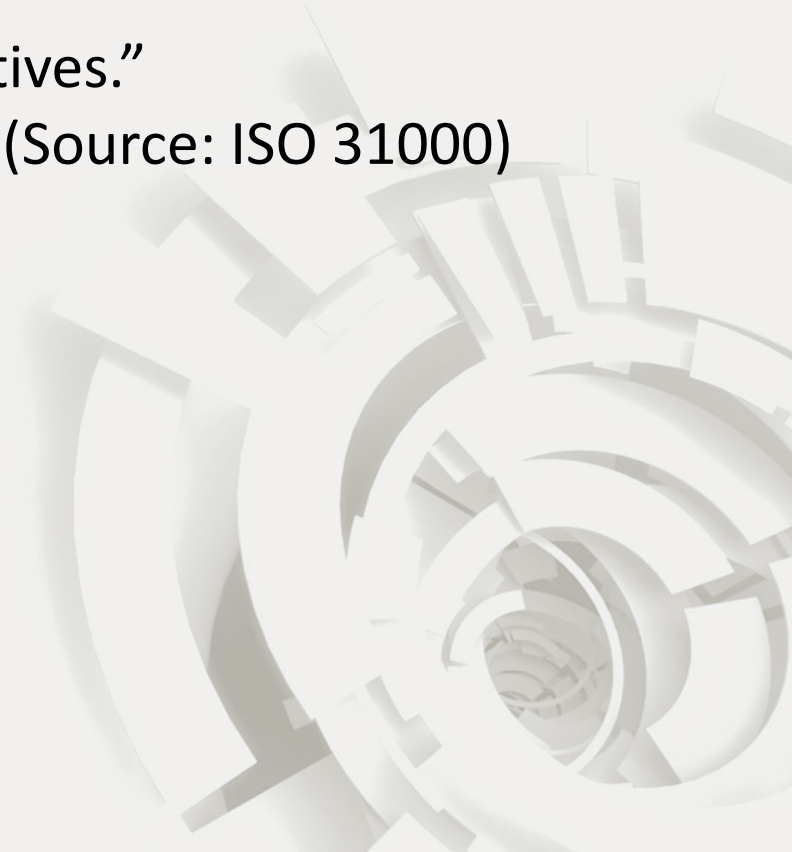


Different Perspectives of “risk”

- **Risk:**

“The effect of uncertainty on objectives.”

(Source: ISO 31000)



Different Perspectives of “risk”

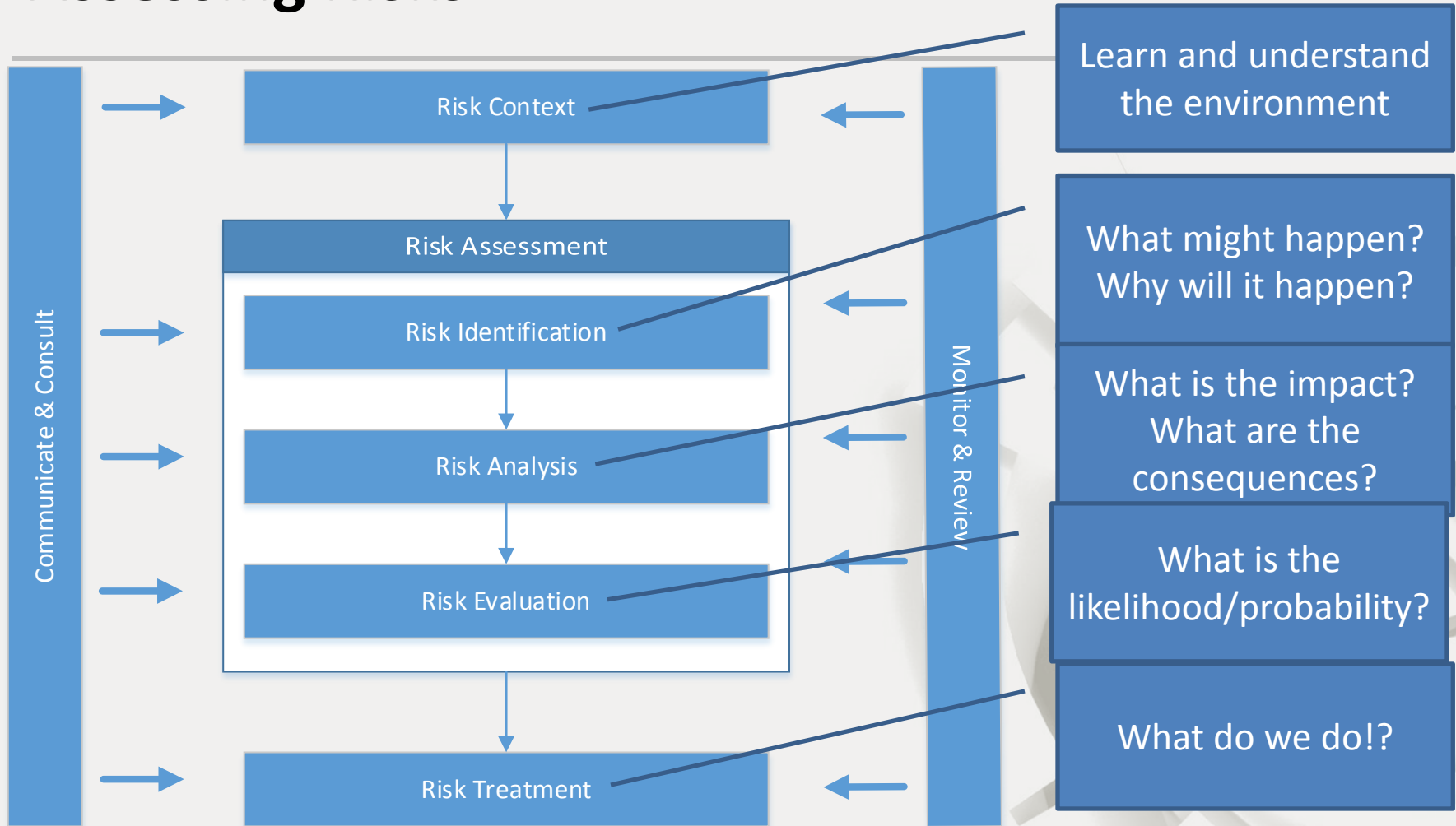
- **Risk:**

“The effect of uncertainty on achievement of objectives. An effect is a deviation from the desired outcome – which may present positive or negative results.”

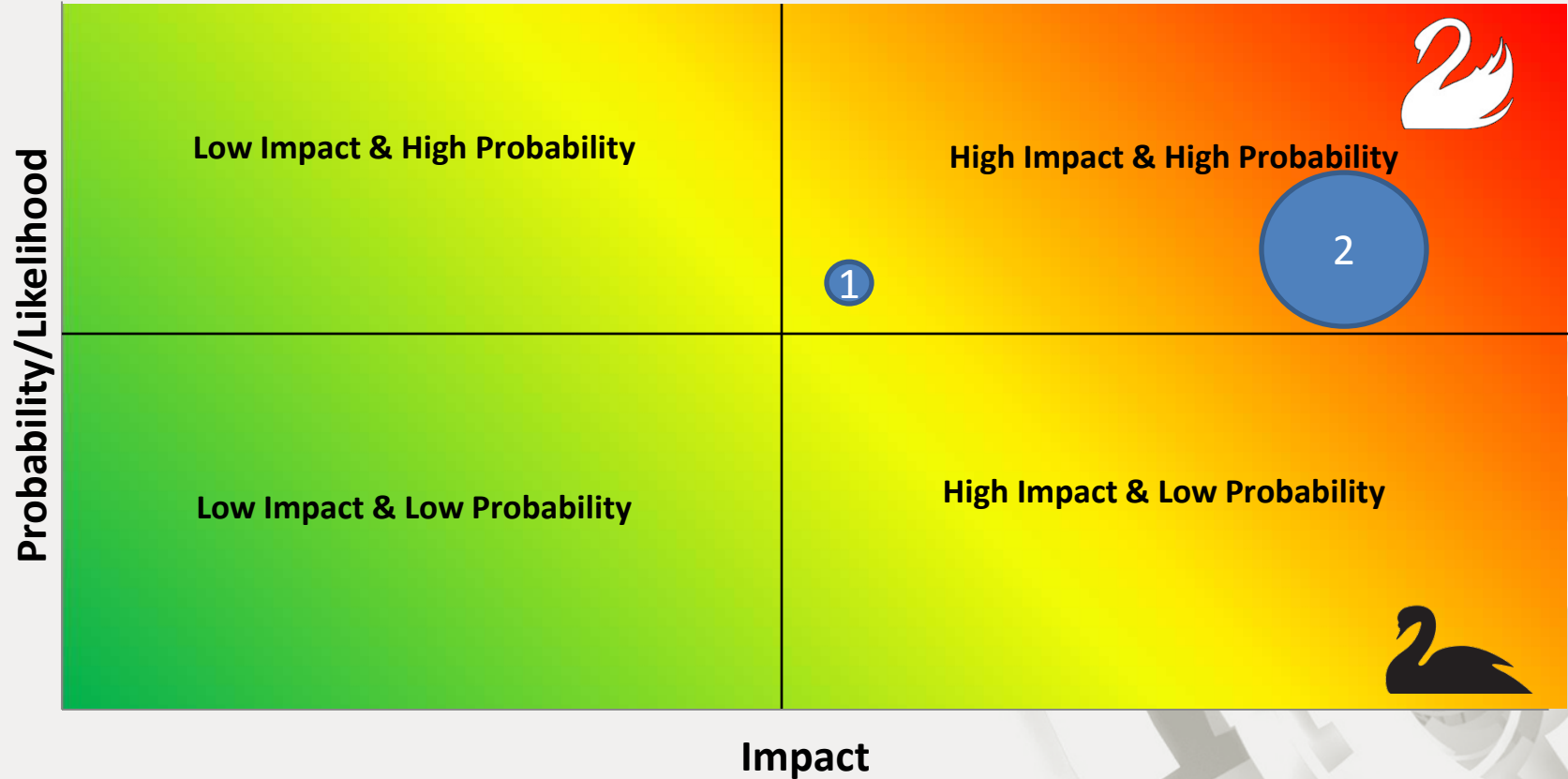
(Source: ERM Playbook)



Assessing Risks



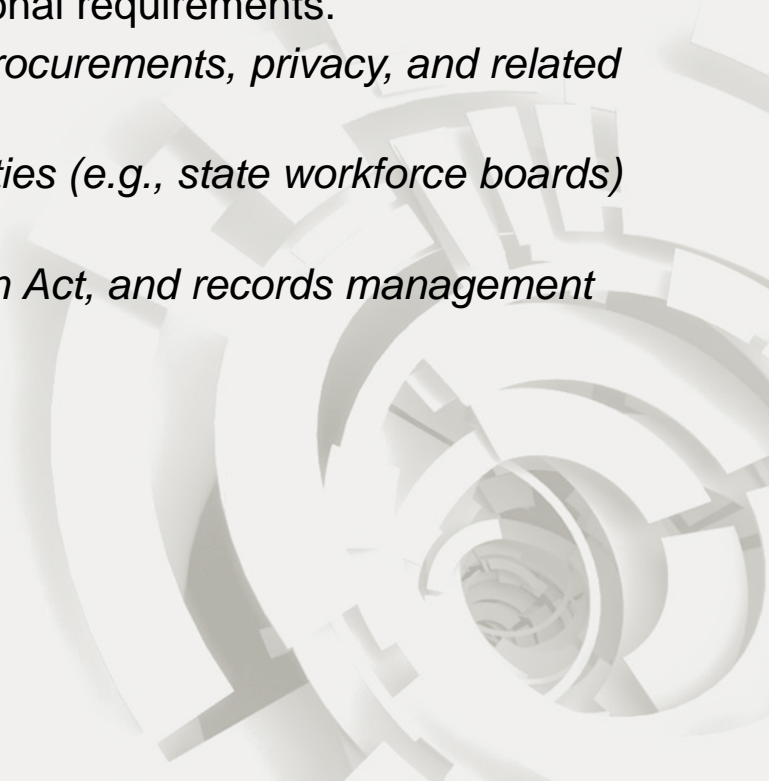
A way to measure risk



What's the Value in Assessing Risk?



Risk Categories: Compliance Risk

- **Compliance:** Failure to comply with applicable laws and regulations; failure to detect and report activities that violate legal or organizational requirements.
 - *Fails to comply with laws and regulations for procurements, privacy, and related issues.*
 - *Agency, grantees, contractors, and related entities (e.g., state workforce boards) do not comply with federal law and regulations.*
 - *Fails to comply with PII, Freedom of Information Act, and records management requirements.*
- 

Risk Categories: Operational Risks

- **Technological:** Risks associated with advances in technology and impacts to operations. Examples:
 - *Employees lack IT resources and skills*
 - *Technology advances make current systems inadequate or obsolete*
 - *Agencies lose data*
- **Resource Management:** Risks to effectiveness, reliability, or quality of products and services due to how agency manages key business processes. Examples:
 - People:** *Fails to hire, develop, and retain talent; not enough staff with appropriate skill sets; lack of succession planning.*
 - Systems and Processes:** *Does not leverage “best practices;” fails to obtain required approvals or clearances; does not execute work, as planned.*
 - Contracts and Grants Management:** *Grants/contracts are not properly planned, awarded, or administered; contractors/grantees do not comply with terms and conditions of awards; awardees fail to achieve program outcomes or provide satisfactory deliverables.*

Risk Categories: Operational (cont'd)

Resource Management, continued

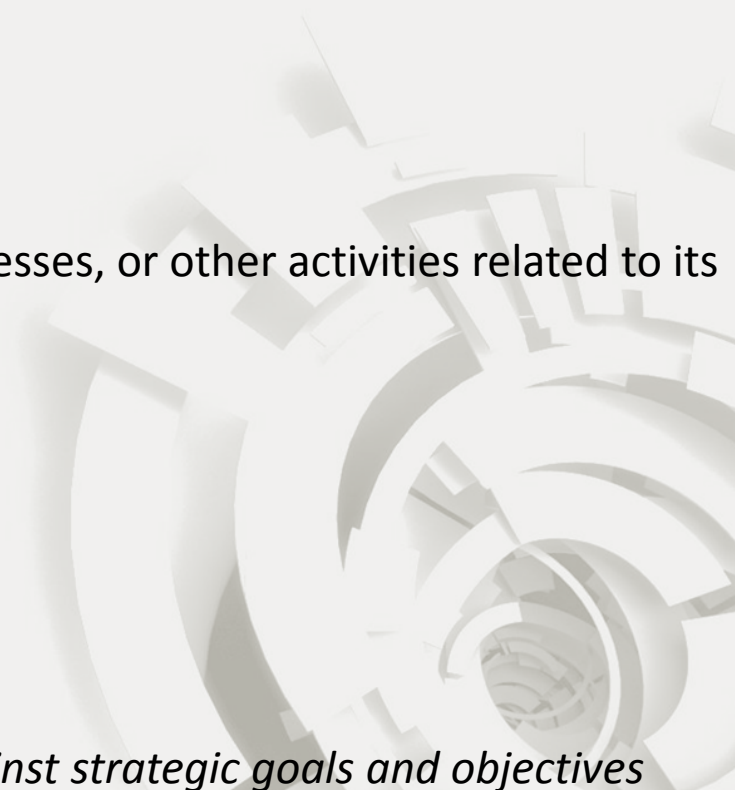
Financial Management: *lacks sound budget planning; fails to follow federal budgeting requirements; submits inaccurate financial reports.*

Policies and Procedures: *lacks current written policies and procedures to guide and clarify key work and core functions; Field office operations are not consistent.*

Physical Assets: *Does not track or monitor major facilities, equipment, or personal property.*

- **Hazard:** Risk that employee or organizational attitudes, conduct, or lack of awareness may impact protection of lives and property, and hinder efforts to prevent accidents and fatal incidents.
 - *Insider threats or personal crimes, including vandalism*
 - *Severe weather events*
 - *“Active” shooter incidents*

Risk Categories: Strategic Risks

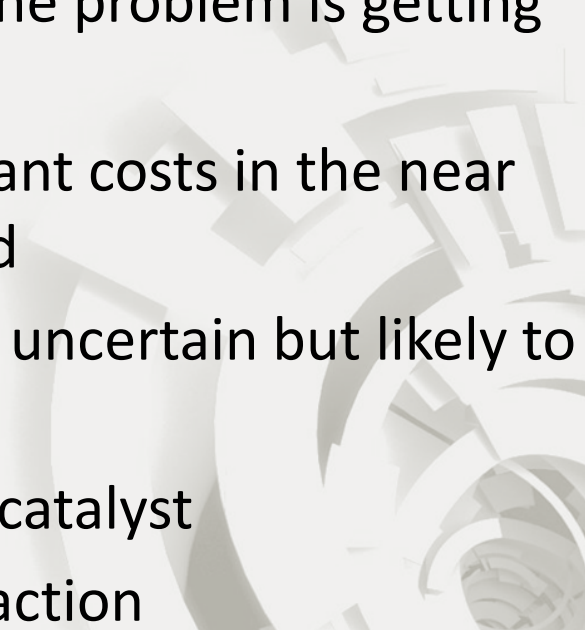
- **Reputational:**
 - *Employee misconduct*
 - *Unfair treatment of employees*
 - *Loss or release of PII*
 - **Political:** Political events may impact goals, processes, or other activities related to its operations. Examples:
 - *Budget cuts by Congress*
 - *Executive Orders, new legislation*
 - *Court Decisions*
 - **Management Risks:**
 - *“Tone at the Top”*
 - *Lack of, or ineffective internal controls*
 - *Effectiveness in managing performance against strategic goals and objectives*
- 

What could prevent us from seeing risks?

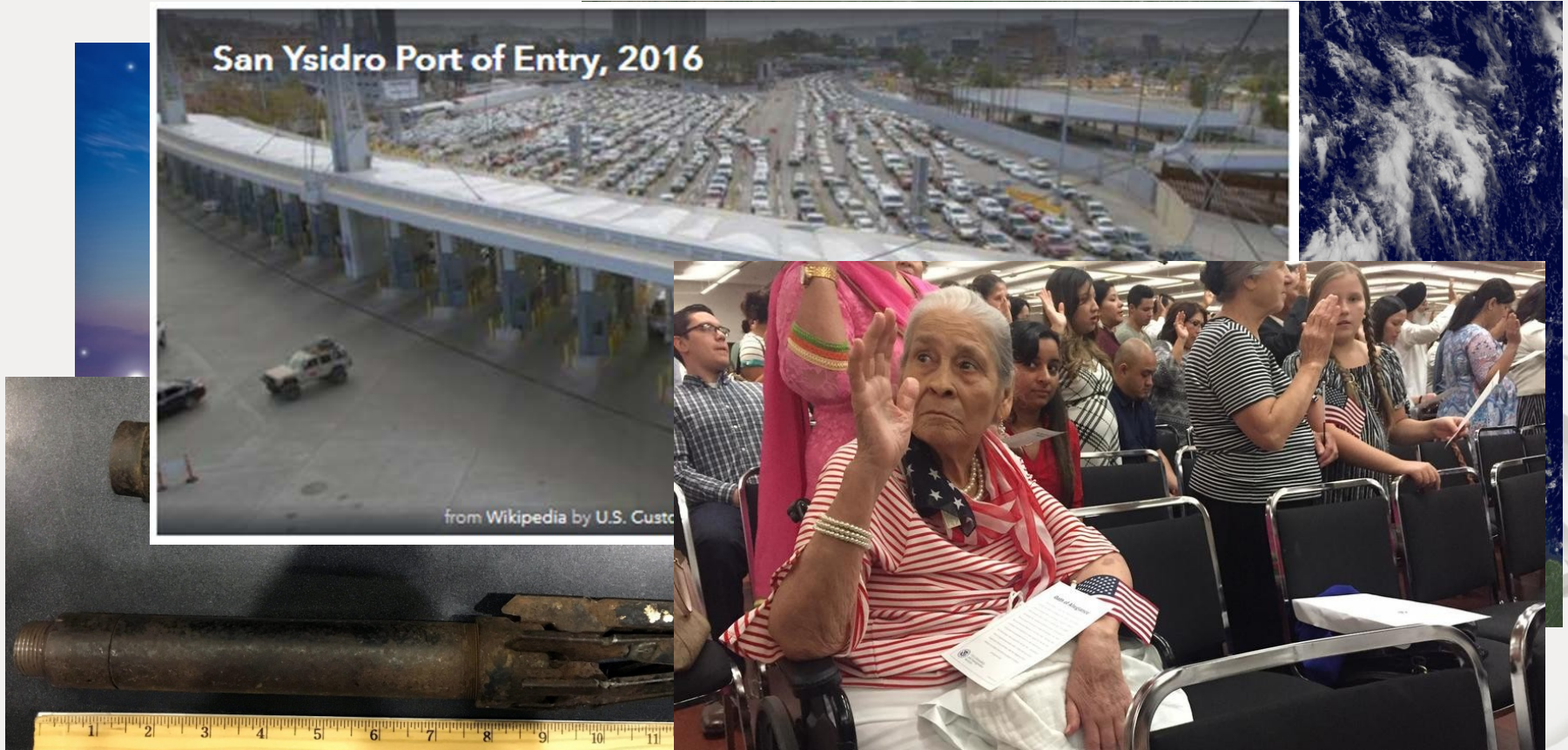
- Some common obstacles could be...
 - Not fully understanding the environment and emerging threats
 - Withholding information because...
 - Knowledge gaps or failure to integrate knowledge
 - Not applying lessons learned
 - Constant churn in key personnel
 - Knowing the risks but not dealing with them



Predicable Surprises

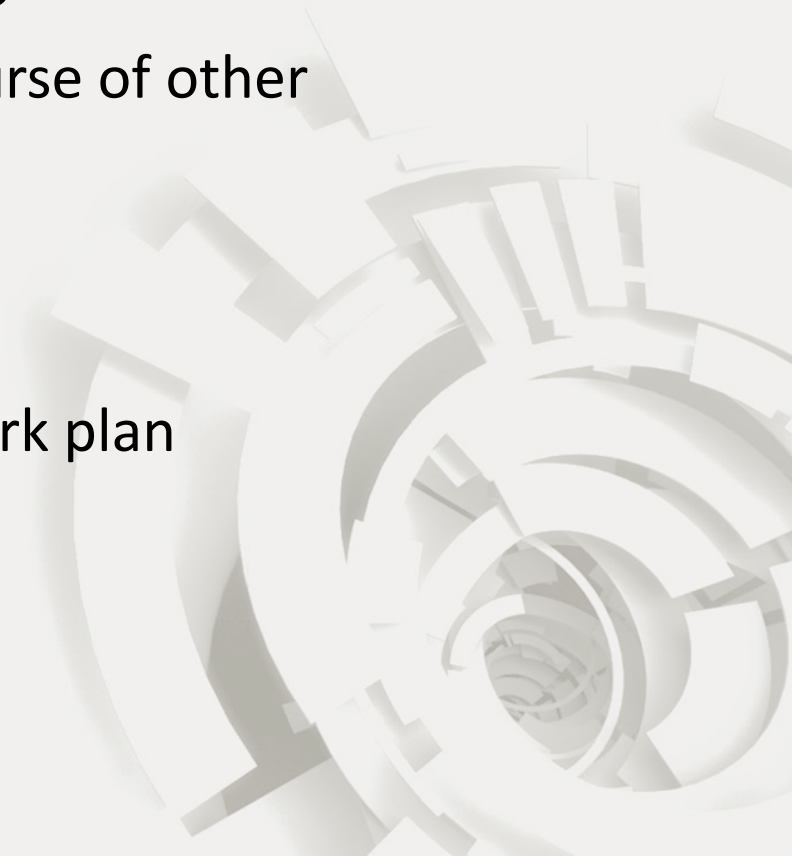
1. Leaders know a problem exists and won't solve it
 2. Organizational members recognize the problem is getting worse
 3. Fixing the problem will incur significant costs in the near term but the benefits will be delayed
 4. The reward of avoiding a cost that is uncertain but likely to be much larger
 5. If it ain't broke, don't fix it– needs a catalyst
 6. A small minority benefits from non-action
- 

What are potential risks that DHS faces?



DHS-OIG Work Planning

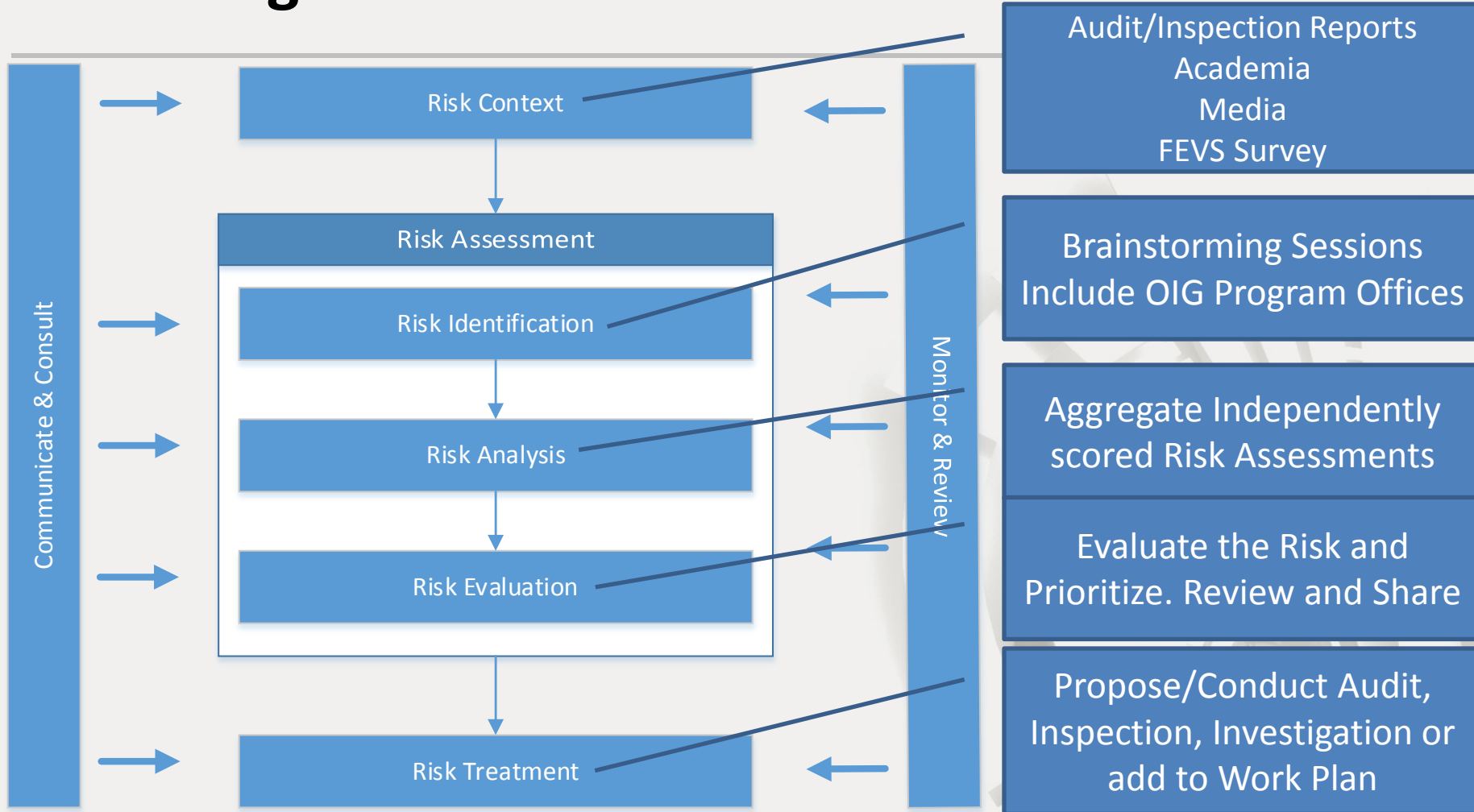
- Generally reactive in the work we do
- Some work identified during the course of other audit/inspection/investigative work
- Congressional requests
- Changes in legislation
- Working towards a **risk informed** work plan



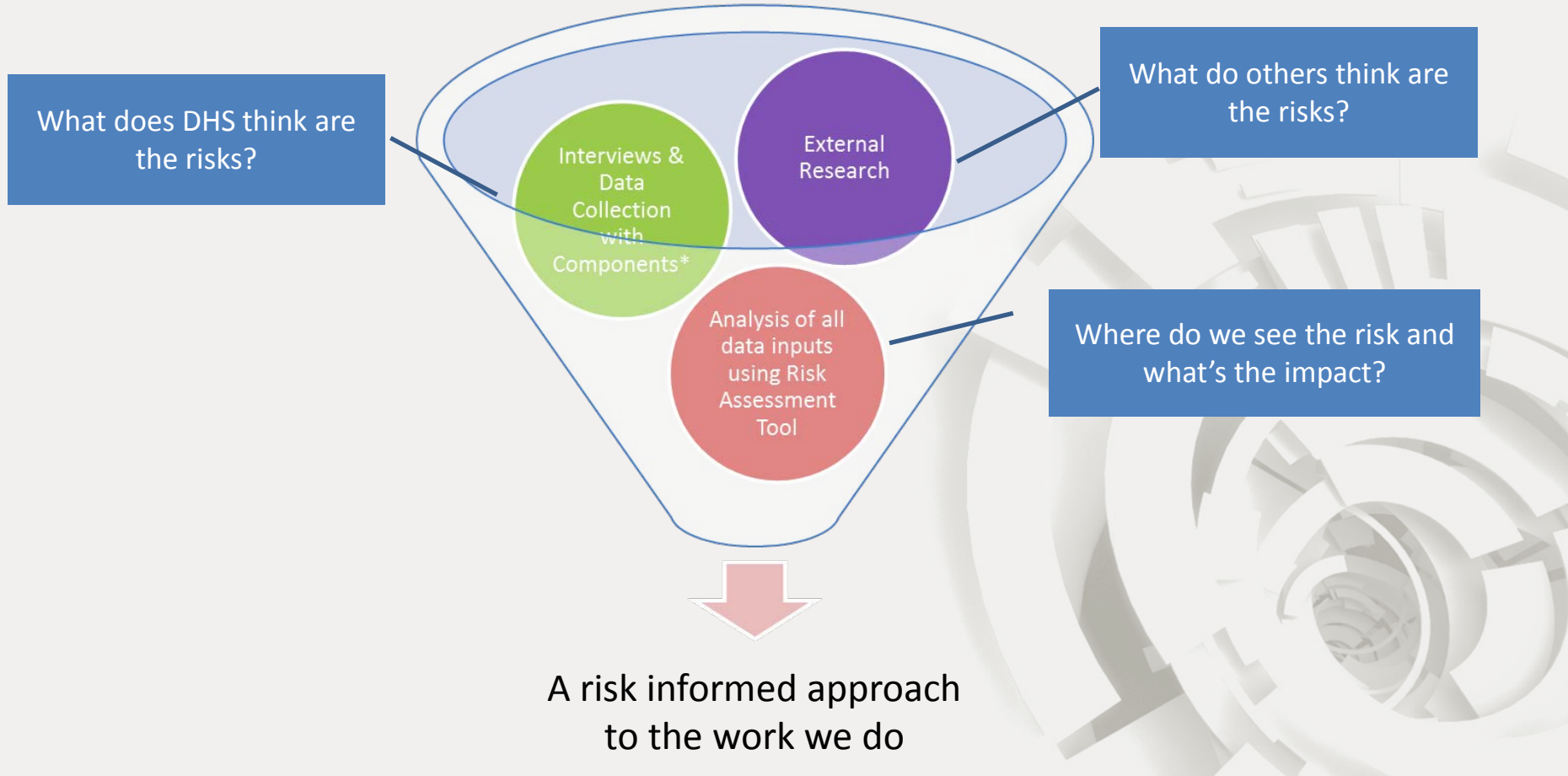
Johari Window Approach – Reducing Unknown-Unknowns

	Known by OIG	Unknown to OIG
Known by Others	Open Arena	Blind Spot
Unknown by Others	Facade	Unknown-Unknowns

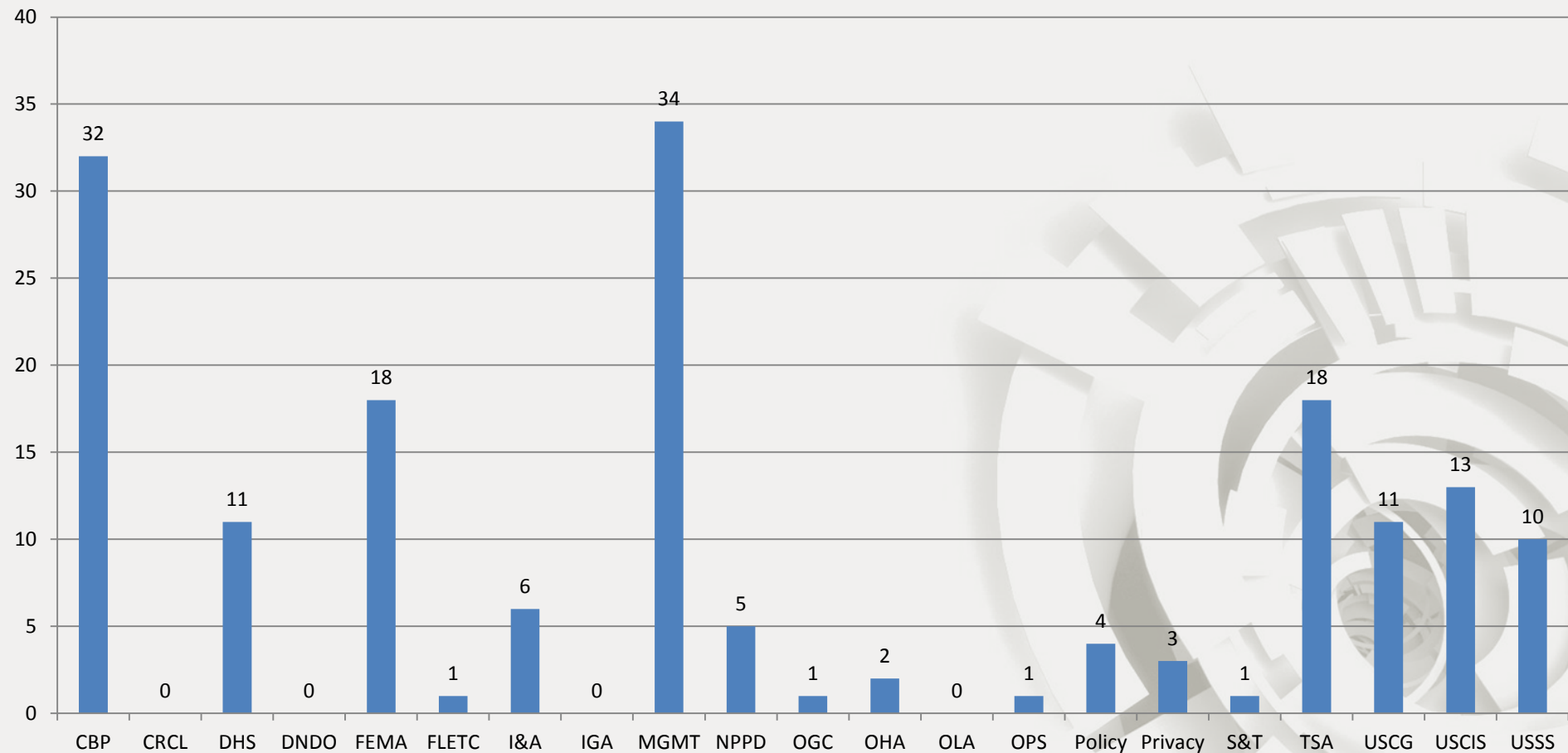
Assessing Risks



Risk Assessment Division



FY15-17 Reports by Component

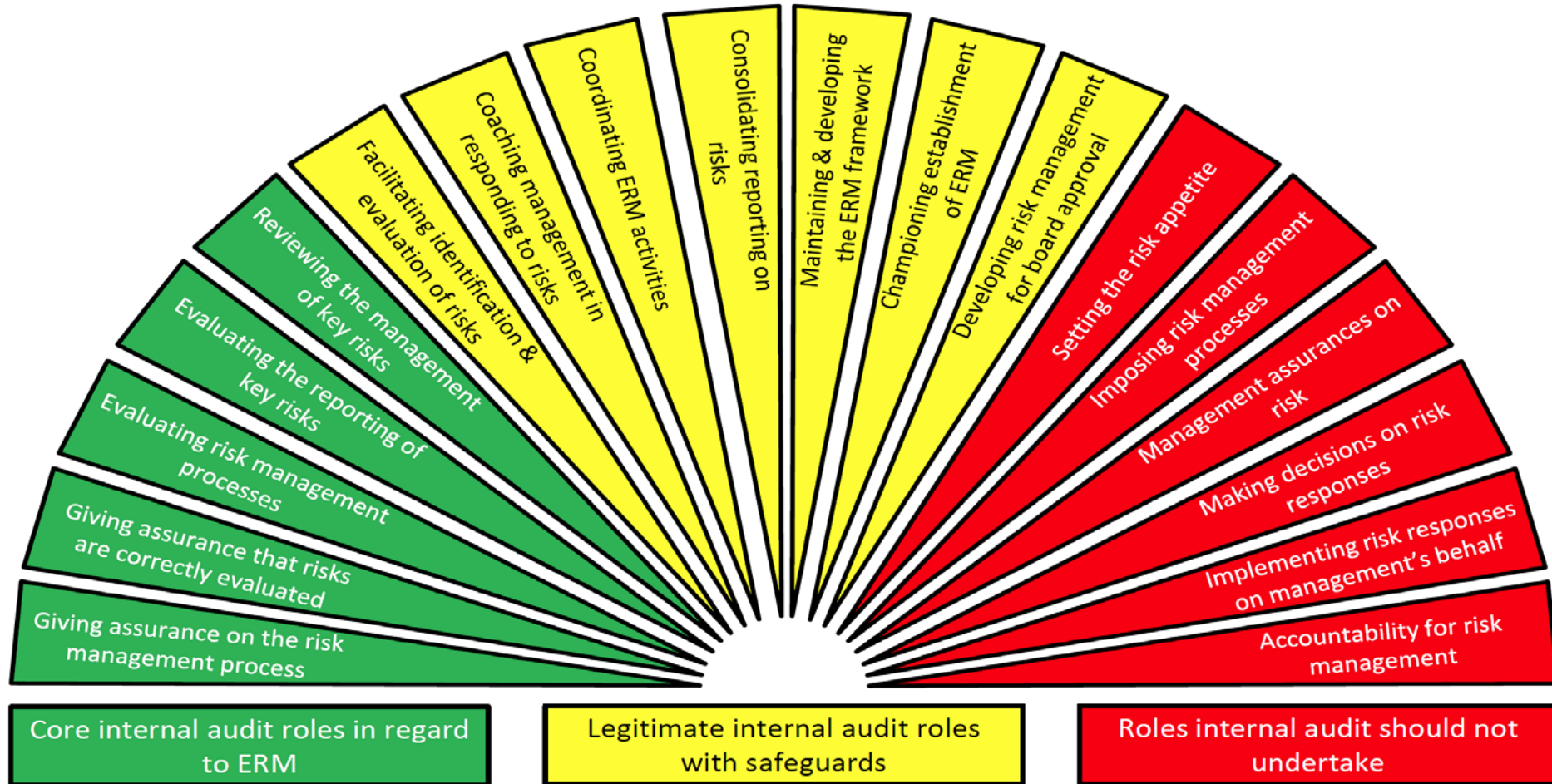


What we are developing to assess risks

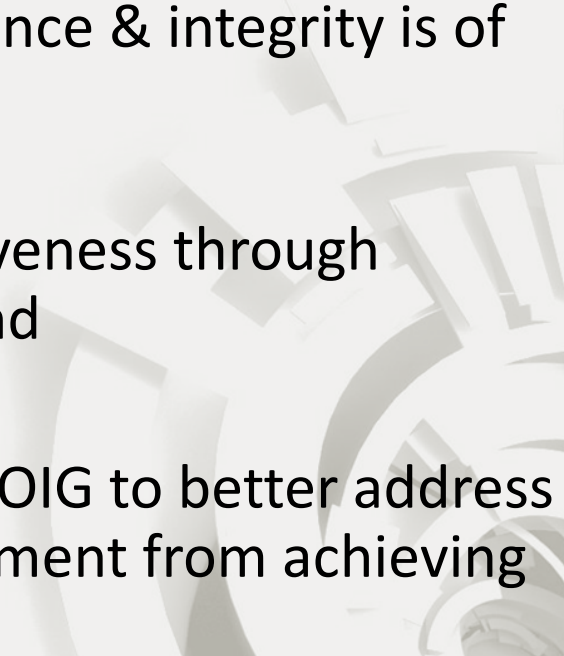
- Legal Authorities
- Resource Maps
- Risk Assessments
- Stakeholder Maps
- Risk Alerts



Internal Audit Risk Roles and Responsibilities



Value Proposition & Benefits

- As an OIG our credibility, independence & integrity is of utmost importance
 - Maximize OIG efficiency and effectiveness through prudent use of limited resources; and
 - Improve communication within the OIG to better address risks that would prevent the Department from achieving its objectives.
- 

Questions

Contact Info:

Name: Shelley Howes

Position: Director, Office of Enterprise Risk Identification and Management

Email: Shelley.Howes@oig.dhs.gov

Phone: 617-869-6879

