

Annual Planning: Creating a Risk-Based Annual Audit Plan

Presented by: Erica Smith

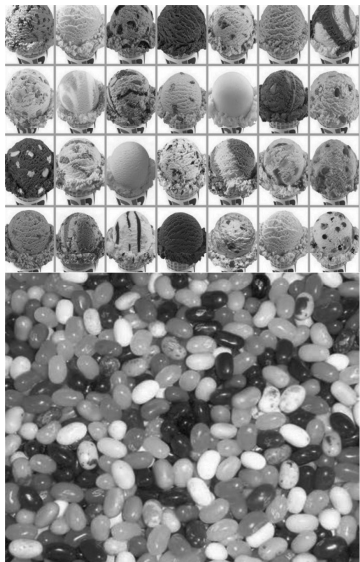
Course Objectives



- Provide an approach to organizational audit planning that focuses an OIG's efforts on those risks that pose the most serious challenges for government entities in maintaining fiscal integrity and operational effectiveness.
- Identify audit activities through which the OIG can add value not provided by other agencies/units.

~~Magic Formula!~~

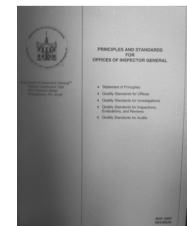
2



Important to remember:

- No two inspector general functions are exactly the same
- No two inspector general audit functions are exactly the same
- Many flavors of inspector general functions

Professional Standards



3

4

GAGAS – Yellow Book



Yellow Book does not require an annual or overall organizational audit plan.

(But it is still a good idea...)

5.12 The audit organization should establish policies and procedures for the initiation, acceptance, and continuance of engagements that are designed to provide reasonable assurance that the organization will undertake engagements only if it

- a. complies with professional standards, applicable legal and regulatory requirements, and ethical principles;
- b. acts within its legal mandate or authority; and
- c. has the capabilities, including time and resources, to do so.

5

IIA – Red Book



“2010 – Planning

The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization’s goals.

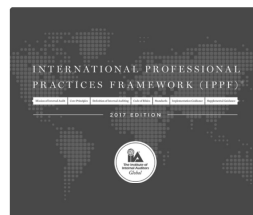


- ★ • 2010.A1 – The internal audit activity’s plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.
- 2010.A2 – The chief audit executive must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions.
- 2010.C1 – The chief audit executive should consider accepting proposed consulting engagements based on the engagement’s potential to improve management of risks, add value, and improve the organization’s operations. Accepted engagements must be included in the plan.”

6

Risk Definition

“The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.”



7

What is a Risk Assessment?

Process of identifying areas within an entity where there is risk of fraud, waste, abuse, inefficiency, and/or ineffectiveness.

- practical
- sustainable
- easy to understand

8

Basic Assumptions

Audits must add value, *monetary or non-monetary*

Audits enhance the *effectiveness* and *efficiency* of an agency

Audits improve the quality of *outputs* and/or *outcomes*

= *Return on Investment*

9

Why do you need a plan?

1. Maximize OIG efficiency and effectiveness
2. Transparency
3. Induce anticipatory correction by agencies
4. Credibility

10

OIG as a Glass House



- Make prudent use of limited resources
 - Personnel hours, dollars, ROI
- Prioritize

Maximize OIG efficiency and effectiveness

11

Is This Familiar?

You are picking on us!

No

You are using audits for your own agenda!

No

Your audits are politically motivated!

No

You are trying to make us look bad!

No



Transparency

12

Spur Pre-emptive Correction



- The OIG auditors are coming!
- Let's fix everything! Maybe then they won't come. Or at least we'll get a clean audit.
- That other unit is getting audited! Let's fix ours fast.

Anticipatory Correction

= easy ROI

13

Planning Can Help Avoid These Questions

Where was the IG?

What was the IG doing instead?

CREDIBILITY

14

Risk-Based Audit Selection Process

Logical

Defensible

Reasonable

System-Driven

No one size fits all.

Information-Driven

Quantifiable

CREDIBILITY

15

What to audit?

The decision on what to audit generally occurs through one or more of the following methods: (GAGAS 5.12)

1. Legislative or regulatory mandate
2. Request by an elected official
3. Request by an agency
4. Risk assessment approach

16



Risk Assessment in Annual Audit Planning

Is...

- A tool for setting audit priorities
- A tool for communicating and justifying audit priorities

Is not...

- Determination of agency risk appetite
- Risk management
- Risk response

Agency
management's
responsibility

GAO's Standards for Internal Control in the Federal Government (Green Book) 2014:

"External auditors and the office of the inspector general (OIG), if applicable, are not considered a part of an entity's internal control system. While management may evaluate and incorporate recommendations by external auditors and the OIG, responsibility for an entity's internal control system resides with management." (OV2.15)

18

Risk Assessment Process

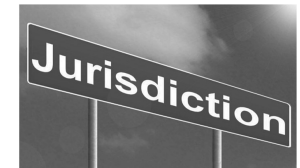
- Step 1: Understand the Universe ★
- Step 2: Identify risks
- Step 3: Develop assessment criteria
- Step 4: Assess risk and risk interactions
- Step 5: Prioritize risk
- Step 6: Develop and execute the risk-based audit plan

Adapted from: Committee of Sponsoring Organizations of the Treadway Commission, *Risk Assessment in Practice*, By Deloitte & Touche LLP, October 2012.

19

Step 1: Understand the Universe

1. Know your jurisdiction



2. Develop Audit Universe



20

Audit Universe

Consider:

Qualitative

- Critical processes and functions
- Quality of life

Quantitative

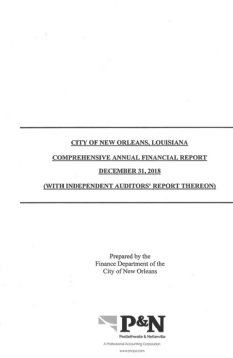
- Dollars and Cents



Consider carefully the correct unit of assessment for your needs: agencies, departments, programs, sub-programs, vendors, grants?

21

In Practice



22

Step 2: Identify Risks

- Prior audits
- Audits in other jurisdictions ★
- Investigations
- Tipline
- Mission statements
- Budget and financial plan
- Strategic plans
- Media articles
- Hearings and proceedings
- CAFR
- GAO's High Risk List
- Management or employee questionnaires
- Informational interviews with agency heads

23

GAO's High Risk List

Every 2 years at the start of a new Congress, GAO calls attention to agencies and program areas that are high risk due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or are most in need of transformation. The 2017 update identified 3 new High Risk areas and removed 1 area. An additional High Risk area was added in January 2018. The update is available below.

View the 2017 Report **Listen to the 2017 Podcast**

2017 LIST **AREA RATINGS** **BACKGROUND** **MULTIMEDIA** **Share This:** [Facebook] [Twitter] [LinkedIn] [Email]

GAO's High Risk List is designating four new High Risk areas:

- Government-wide Personnel Security Clearance Process (added January 2018),
- Improving Management of Federal Programs that Serve Tribes and Their Members,
- U.S. Government's Environmental Liabilities,
- 2020 Decennial Census.

GAO removed one area from the High Risk List. Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland.

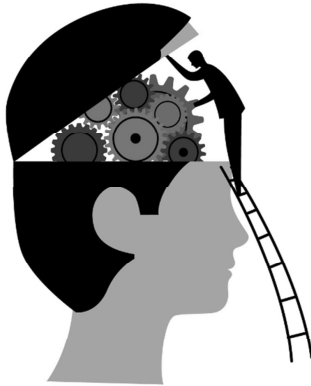
This brings our current High Risk List to a total of 35 areas.

GAO's 2017 High Risk List:

Sort By Title	Sort By Topic
Government-wide Personnel Security Clearance Process — NEW	Government Operations
Improving Federal Management of Programs that Serve Tribes and Their Members — NEW	Government Operations
U.S. Government's Environmental Liability — NEW	Government Operations

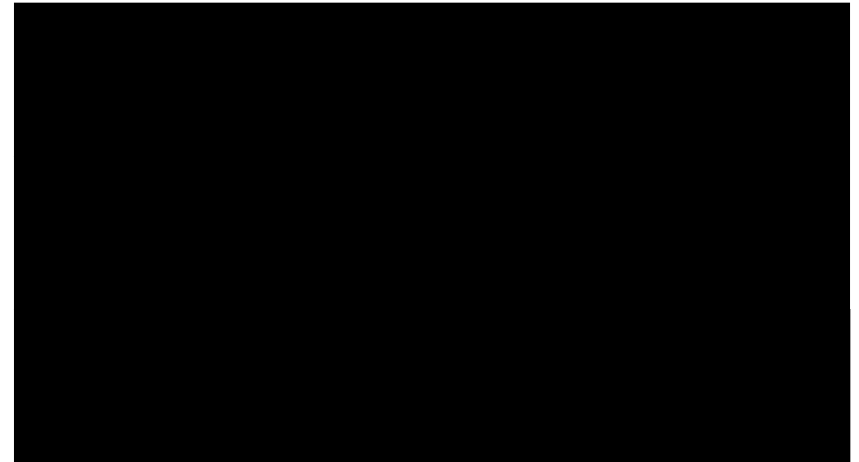
24

Obtain an Understanding!



25

Wiley E. Coyote V. Road Runner



26

What's the strategy?



Ask: How will future staff or my future self be able to find and use this information?

27

Questionnaires

If you use questionnaires, consider different questionnaires for different audiences

- Management
- Elected or appointed officials
- Front-line employees
- Public



Plan for effective questionnaire design

- How to maximize responses?
- How to efficiently analyze responses?
- How write questions that elicit decision-useful information?



28

Examples of Questions

- What is the Purpose/Mission/Objective of your work unit?
- What are the primary strengths of this unit?
- What obstacles do you see that affect your goals and objectives?
- If you had additional resources to help you achieve your objectives, what would they be?
- What is the worst thing that could happen in your unit?
- What is the worst thing that has already happened in your unit?
- What are some other units that are critical to your mission, and which give you the most concern (and why)?

29

Step 3: Develop Assessment Criteria

Risk Factor



Likelihood



Impact



30

Definitions

Risk Factor

- A condition or characteristic that increases the probability or severity of a negative outcome. ★

Likelihood

- The probability of a negative outcome occurring.

Impact

- A negative outcome that would impair an agency's ability to achieve its objectives.

31

Risk of what?



Risk to whom?

High Risk Area!!!

32

Consider inherent and residual risks

Inherent risk - Nature of the entity and its environment, absent any internal controls

- Sky diving
- Climbing Mount Everest
- Large sums of cash payments

33



Consider inherent and residual risks

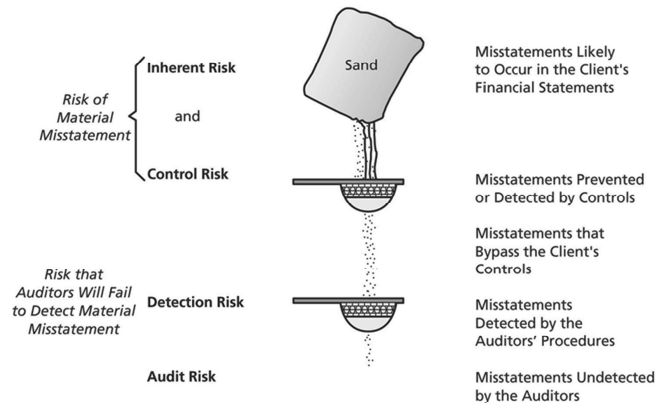
Residual risk - Remaining after agency's action/inaction (if controls effectively designed and implemented)

- Given an effective parachute
- Guided by experienced Sherpas
- If controls are properly designed and operating effectively

35



Consider inherent and residual risks



37

Examples of Risk Factors



- High volume of financial transactions, or large amount of money involved
- Weak security system
- Numerous prior audit findings not corrected
- Recent leadership change
- No performance measurement
- Weak supervisory structure
- Lax recordkeeping
- New IT systems
- Very large or very small number of personnel



38

Risk Factor Identification

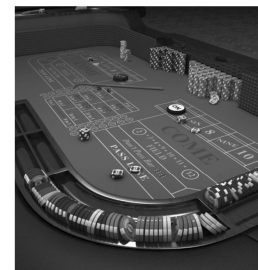
Identify and select a manageable number of risk factors most likely to lead to risk consequences, based on the entity's objectives.

High Level Category	Risk Factor	Indicator Definition
Financial Risk	Financial Risk	The risk of financial insolvency or instability, or fraud, waste, or abuse involving the financial transactions or reporting of the entity.
	Fraud Risk	The risk of theft, fraud, or corruption within the entity.
	Physical Asset Risk	The risk that physical assets of the entity are not adequately managed, maintained, or safeguarded.
Compliance Risk	Legal/Compliance Risk	The risk that the agency is not complying with local, state, or federal laws, regulations, or professional standards.
Operational Risk	Management Risk	The risk that the organization has improper or insufficient management/oversight.
	Process Risk	The risk that the entity lacks updated, well-documented policies and procedures to achieve the entity's mission.
	Staffing Risk	The risk that the entity does not have the right people in the right places with the right skills to achieve the entity's mission.
	Technological Risk	The risk of technological failures within an entity.
Reputational Risk	Political Change/Strategic Planning	The risk that the political climate and/or legislative changes may have adversely affected the entity and lack of strategic plan and/or the inability to effectively implement strategic planning initiatives.

39

Define Assessment Criteria

Likelihood



Define and assign points for each impact

Low	1 point
Medium	5 points
High	10 points

Risk factor: **Technological Risk**

Likelihood

Low = Last upgrade < 1 year ago
 Medium = Last upgrade 1-5 years ago
 High = Last Upgrade > 5 years ago

40

Define Assessment Criteria

Impact

Define and assign points for each impact



Minor	1 point
Moderate	5 points
Extreme	10 points

Risk factor: **Technological Risk**

Impact

Minor = Disruption of services for one day or less

Moderate = Disruption of services for 2-7 days

Extreme = Disruption of services greater than 7 days

41

Step 4: Assess Risk & Risk Interactions

1. Assign a likelihood and impact score.
2. Assign a weight to each factor to reflect relative importance.
3. Rate each auditable unit, including an adjustment based on staff judgment, experience, or additional information if appropriate.

	Likelihood	Impact	Score	Weight	Weighted Score
Financial Risk (30%) (Monetary and Asset Values)	5	x 10	= 50	x 30%	= 15.00
Compliance (20%) (Legal and Regulatory)	10	x 10	= 100	x 20%	= 20.00
Operational (40%) (Processes, Management, Staffing, and Technology)	10	x 10	= 100	x 40%	= 40.00
Reputational (10%) (Political environments, and Community Outreach Strategies)	5	x 5	= 25	x 10%	= 2.50
Total Score					77.50

42

Step 5: Prioritize Risk

Rank it!

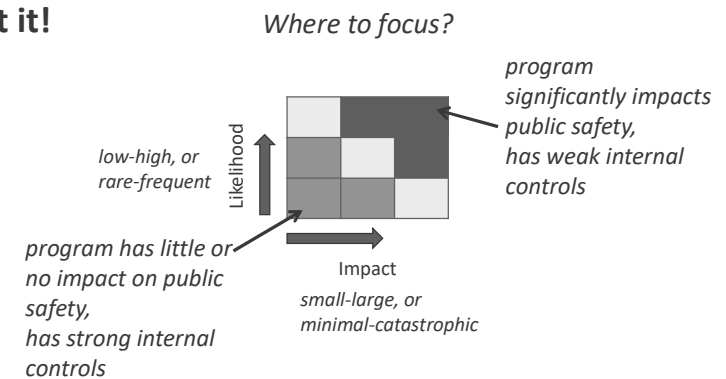
Sheet Name	Agency Name	2017 Actual Budget	2017 FTEs / Budgeted Positions	2018 Adopted Budget	Financial (30%)	Compliance (20%)	Operational (40%)	Reputational (10%)	Total
1 OPSO	OPSO	Unknown	Unknown	\$ 53,188,976.00	30	20	40	10	100
2 SWB	Sewerage and Water Board	\$ 327,105,015	1300-1800	\$ 287,277,088.00	30	14	40	10	94
3 SWB, Rev	Sewerage and Water Board- Revenue	\$ 327,105,015	1300-1800	\$ 287,277,088.00	30	14	40	10	94
4 OPCD	Orleans Parish Comm. District	\$ 15,596,960	143	\$ 16,431,113.00	21	14	40	7	82
5 Public Works	Public Works	\$ 45,827,888	202	\$ 53,116,255.00	15	20	40	2.5	77.5
6 OPCD, Rev	OPCD- Revenue	\$ 15,596,960	143	\$ 16,431,113.00	21	14	20	10	65
7 Sanitation, Service Charges	Sanitation - Service Charges	\$ 36,854,237	N/A	\$ 34,165,170.00	21	6	28	7	62
8 NOEA, Rev	NOEA- Revenue	\$ (10,600,946)	140	\$ (6,102,866.00)	24	10	20	14	62
9 IT and Innovation	IT	\$ 11,996,579	53	\$ 11,805,517.00	15	10	28	5	58
10 Red Signal Light	Red Signal Light/Camera Enforcement - Fines	\$ 24,000,000	N/A	\$ 25,200,000.00	14.7	7	28	7	56.7
11 Finance-Finance	Finance - Finance	\$ 8,336,748	8	\$ 2,609,593.00	21	7	19.6	3.5	51.1
12 Finance-Procurement	Finance - Procurement	\$ 494,565	10	\$ 520,278.00	10.5	14	19.6	7	51.1

Score Ranking	
Low (1-30)	
Medium (31-69)	
High (70-100)	

43

Risk Matrix

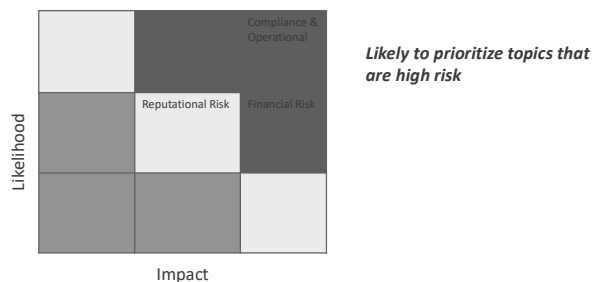
Plot it!



44

Risk Matrix, contd.

You may wish to illustrate where specific risks fall by plotting them according to their specific impact & likelihood scores.



45

Step 6: Develop the Risk-Based Audit Plan

Process:

- Gather ideas
- Review risk assessment
- Hold planning meeting (with audit staff, leadership, IG, others?...)
- Draft plan
- CAE, IG, audit committee, approves plan



Share plan (with your staff, board, agency, public?...)

46

Step 7: Execute the Plan

Can we do something not on the plan?

What if we don't do everything on the plan?

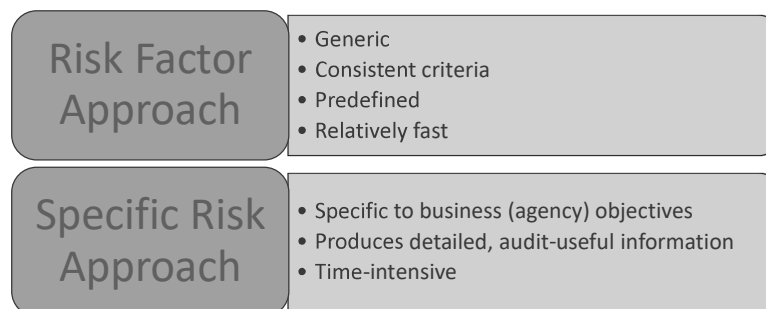
What if the agency already fixed the problem?

Remember why you have a plan:

- Maximize OIG efficiency and effectiveness
- Transparency
- Induce anticipatory correction by agencies
- Credibility

47

Two Other Approaches to Identifying Risk Factors



Adapted from: Rick A. Wright, Jr., *The Internal Auditor's Guide to Risk Assessment*, Institute of Internal Auditors Research Foundation, 2013.

48

You need more than Risk Scores... ★

Consider other prioritization criteria:

- High public interest/concern
- High concern to public officials
- Agency requested
- Will help OIG gain knowledge of a new area
- Ensure coverage across all areas
- OIG is uniquely positioned to audit it (e.g., access to information not available to other entities)

Where will OIG add value?

49



Always Planning

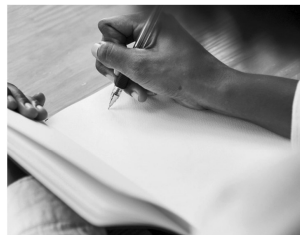
Planning is continuous, not once a year

Always be gathering new audit ideas

- Research & communication
- Effective knowledge management

Write up the ideas

- Use a template
What we know, what we don't know, preliminary risk score
- Compare new ideas to plan: what's next?



51

Final Questions To Ask In Audit Selection Process



Will the audit identify monetary or non-monetary benefits?



Will the audit help the agency attain its objectives?



Do we have the necessary staff resources/expertise?



What is the return on investment?

52



Questions? Comments?

Presented by:

Erica Smith

Deputy Inspector General – Audit and Review
Office of Inspector General – City of New Orleans
504-681-3210
esmith@nolaog.gov