IT Audit Plan Formulation and Stakeholder Engagement

Lisa Siedzik, CISA, IAP, MBA

Agenda

- Introduction
- Learning Objective
- Discussions and Exercises
- Final tips & takeaways

Introduction

Rules

- No idea is a bad idea.
- Be creative.
- Take risks.
- Ask Questions.

Learning Objective

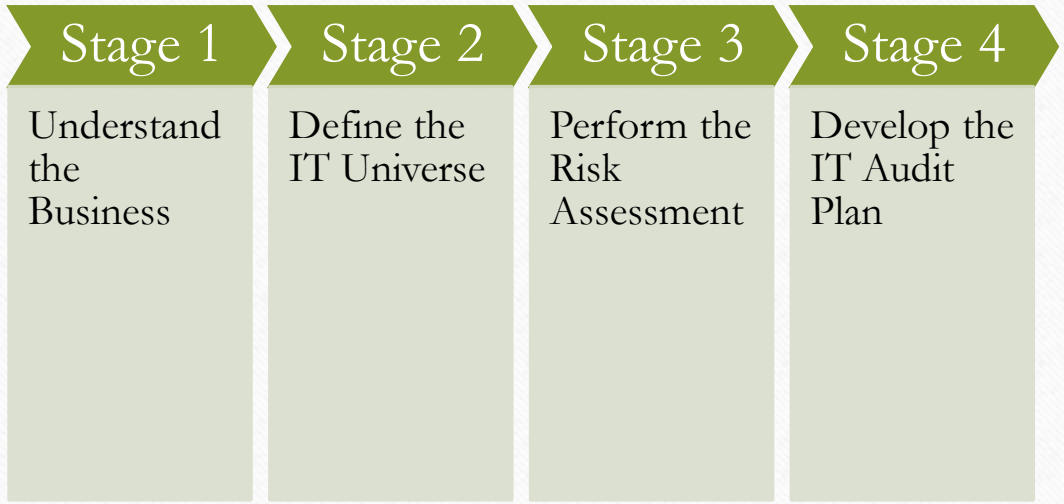
How to formalize the IT audit plan and include in the enterprise audit plan.

How to engage management and executive leadership

Risk Assessment Methodology

RECAP

Process Summary



Questions about any of the following?

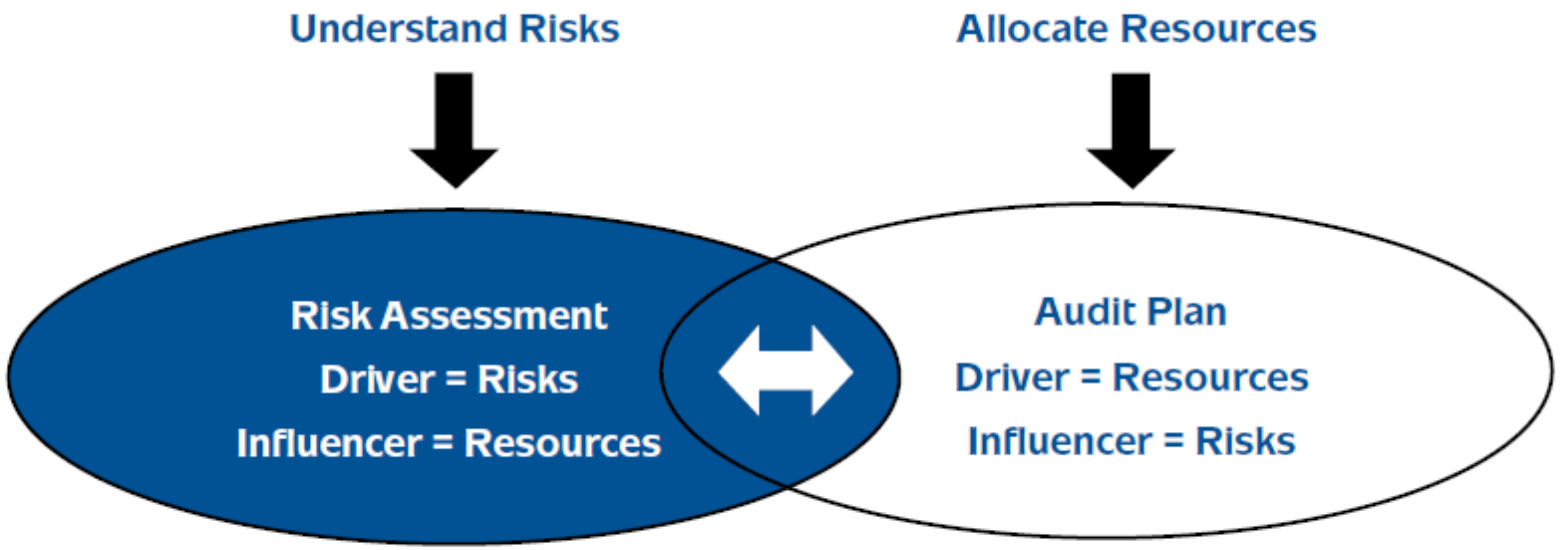
- Risk assessment resources
- IT frameworks
- IT universe development
- Risk factors
- Risk ranking

Formulizing the Audit Plan

Basic Concept

- Objective is to review high risk areas through the allocation of available resources
- Incorporate in audit function's strategic planning
- 'Plan, Do, Check and Act'
- Should include list of audit activities as well as timing, dependencies and resource allocation to reach audit goals
- Typically, and required by red book, is developed by CAE

OBJECTIVES FOR RISK ASSESSMENTS AND AUDIT PLANS



Key Activities

- Obtain explicit input from stakeholders.
- Identify relevant risks.
- Assess risks.
- Prioritize risks.

Key Activities

- Understand universe of potential audits subjects.
- Allocate and rationalize resources.
- Reconcile and finalize the audit plan.

Standards

- GAGAS 1.14 'All GAGAS engagements begin with objectives…' sort of implied…
- IIA Standard 9.4 – Audit Plan
- IIA Standard 10.1 - Budget
- IIA Standard 10.2 – Resources

IIA 9.4 Audit Plan

The chief audit executive must create an internal audit plan that supports the achievement of the organization's objectives.

The chief audit executive must base the internal audit plan on a documented assessment of the organization's strategies, objectives, and risks. This assessment must be informed by input from the board and senior management as well as the chief audit executive's understanding of the organization's governance, risk management, and control processes. The assessment must be performed at least annually.

The internal audit plan must:

- Consider the internal audit mandate and the full range of agreed-to internal audit services.
- Specify internal audit services that support the evaluation and improvement of the organization's governance, risk management, and control processes.
- Consider coverage of information technology governance, fraud risk, the effectiveness of the organization's compliance and ethics programs, and other high-risk areas.
- Identify the necessary human, financial, and technological resources necessary to complete the plan.
- Be dynamic and updated timely in response to changes in the organization's business, risks operations, programs, systems, controls, and organizational culture.

The chief audit executive must review and revise the internal audit plan as necessary and communicate timely to the board and senior management:

- The impact of any resource limitations on internal audit coverage.
- The rationale for not including an assurance engagement in a high-risk area or activity in the plan.
- Conflicting demands for services between major stakeholders, such as high-priority requests based on emerging risks and requests to replace planned assurance engagements with advisory engagements.
- Limitations on scope or restrictions on access to information.

The chief audit executive must discuss the internal audit plan, including significant interim changes, with the board and senior management. The plan and significant changes to the plan must be approved by the board.

IIA 10.1 Financial Resources Management

The chief audit executive must develop a budget that enables the successful implementation of the internal audit strategy and achievement of the plan.

The budget includes the resources necessary for the function's operation, including training and acquisition of technology and tools. The chief audit executive must manage the day-to-day activities of the internal audit function effectively and efficiently, in alignment with the budget.

IIA 10.2 Human Resources Management

The chief audit executive must establish an approach to recruit, develop, and retain internal auditors who are qualified to successfully implement the internal audit strategy and achieve the internal audit plan.

The chief audit executive must strive to ensure that human resources are appropriate, sufficient, and effectively deployed to achieve the approved internal audit plan. *Appropriate* refers to the mix of knowledge, skills, and abilities; *sufficient* refers to the quantity of resources; and *effective deployment* refers to assigning resources in a way that optimizes the achievement of the internal audit plan.

The chief audit executive must communicate with the board and senior management regarding the appropriateness and sufficiency of the internal audit function's human resources. If the function lacks appropriate and sufficient human resources to achieve the internal audit plan, the chief audit executive must determine how to obtain the resources or communicate timely to the board and senior management the impact of the limitations.

IT Audit Plan

- It's one piece of the overall internal audit plan
- It will require internal discussions and reviews before being added to the plan

Traditional Audit Approach	Agile Audit Approach
Audit Plan	**Audit Plan**
• Prescriptive • Hierarchical socialization process – many reviews • Internal audit does not consistently solicit the feedback of business owners on audit scope	• Flexible, allowing broader coverage • Value-added focus • Active business owner's involvement
Audit Fieldwork	**Audit Fieldwork**
• Preassigned team members – focus area • Fieldwork/testing in scope with limited exceptions • Project lead accountable – budget and project timeline • Independent scope area performance • "Findings" validated through status meetings	• Integrated fieldwork execution • Assign focus area by sprint backlog • Discussing roadblocks via daily scrum • Scrum lead accountable – efficiency and value • Focused sprint – efficient delivery • Feedback and reconsideration post every sprint
Review	**Review**
• Hierarchical audit report writing process – various levels and reviews • Robust and detailed audit report • Business owner review almost finalized report • Audit opinion basis facts and activities during scope period	• Sprint retrospectives – consolidation of previous insights • Review completed work with stakeholders • Streamlining and drafting report collaboratively • Consolidation of viewpoints and future insights in audit report

A step further…

Area	Score	Risk Level	Timeline	Audit Days Allocated
IT Infrastructure Configuration Management	37	High	Q1	175
Network Administration and Security	36	High	Q1	150
Windows Server Administration and Security	36	High	Q2	150
Payroll Application and General Controls	35	High	Q3	120
SAP ERP Application and General Controls	34	Medium	Q2	100
OS400 Server Administration and Security	33	Medium	Q2	90 (Outsourced)
Oracle Database Administration and Security	30	Medium	Q4	85 (Outsourced)
Corporate Privacy Compliance	25	Low	Q2	60 (Outsourced)
Major Capital Projects	24	Low	Q2	60
IT Governance Practices	24	Low	Q4	60
Internal Controls Testing & Reporting	N/A	N/A	Q3, Q4	100
Follow-up on Findings	N/A	N/A	Q3, Q4	85

Considerations

In conjunction with the outcome of the IT risk assessment…

- Are there management requests? Consider asking during Stage 1.
- What would the audit frequency be for audits identified? Do you have a rolling 6 month, annual or multi-year plan?
- Can you even perform annual reviews over the audit area based on resources?
- Sourcing strategies. Will you need to outsource any audits? Is it in the budget?
- Sufficient IT resources. Do you have the technical skillset and availability?
- Regulatory and compliance requirements. Are there specific audits that have to be performed annually?

Discussion: What other considerations can you think of?

Frequency Suggestions

	Priority	Frequency	Resource Allocation
H	Immediate action, usually within the first year	Annual reviews or multiple actions within the cycle	High allocation
M	Mid-term action within the audit cycle	One or several audit engagements within the cycle; could be postponed	Base allocation
L	Audit engage-ments usually not planned within the cycle	At most one audit engagement planned within the cycle	Limited allocation

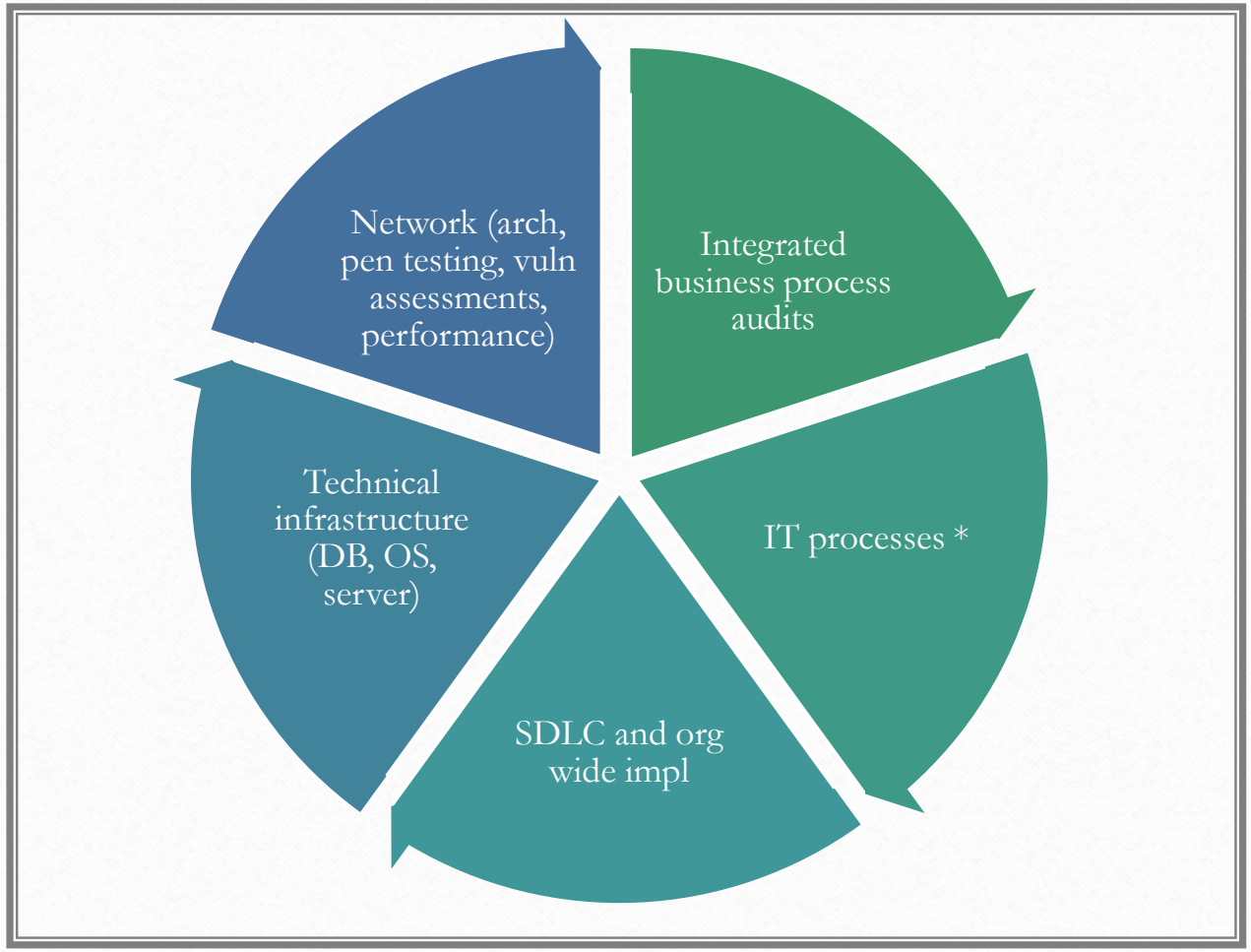
Audit Plan Principles – In Sum

Planning should be consistent with the charter

Activities should be capable of accomplishment within budget and time allotment

Include work schedule with planned dates and estimated time

Prioritized based on last audit engagement, management requests, trending issues, major changes to the business, changes in staff



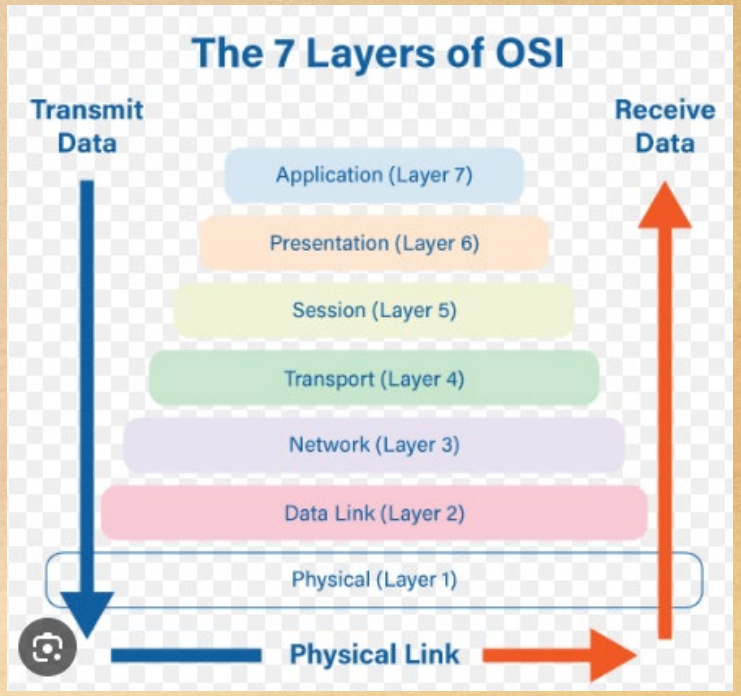
IT Audit Plan Content

* governance, PM effort, software development, policies/procedures, framework processes, information security, cybersecurity, incident management, change management, patch management, help desk

Considerations

To ensure appropriate coverage…

- Contributions to operational, financial and compliance reviews
- Main control objectives (i.e., SOD, cybersecurity)
- Emerging trends and their threats and impacts (Think AI!)
- Think back to yesterday and the manner of attacks on the public sector!



Exercise

1. Objective is to develop an IT audit plan based on the provided information
2. Complete the audit plan based on the information provided

Engagement	Risk Level	Cycle	Audit Days Allocated

*Note: for any recurring engagements or management requests note them by an *.*

Engagement	Risk Level	Cycle	Audit Days Allocated
Penetration Test Coordination	*	0	40
Procurement Application Follow-up	*	0	20
ERP Application & General Controls	H	1	100
Facility 3: HR/Payroll Application	H	2	30
Employee Benefits Apps (Outsource)	H	3	100
Facility 3: IT Infrastructure	H	2	90
UNIX Administration and Security	M/H	1	90
Corp. Privacy Compliance	M/H	3	40
Windows Server Administration and Security	M	3	90
Facility 1: IT Infrastructure	M	3	90
Facility 1: Process Control Systems	M	3	90
Environment Reporting Systems	M	3	30
Major Capital Investment Projects	M	3	30
Sarbanes-Oxley Sustainability	M/*	3	120
ITIL Deployment Practices	L/*	4	40
Total			1000
* Management Request			

Integrating the IT Audit Plan

Audit Universe	Low-integrated Audit Plan	Partially Integrated Audit Plan	Highly Integrated Audit Plan
Business Processes • Operational • Financial • Compliance	Non-IT audit	Non-IT audit	Integrated approach
Applications Systems • Application controls • IT general controls	IT audit	Integrated approach	Integrated approach
IT Infrastructure Controls • Databases • Operating systems • Network	IT audit	IT audit	Integrated approach

Validating the Audit Plan

01

Review to ensure it's a value add for the organization and the audit function

02

Ensure the plan is balanced through the entire cycle with no specific concentration in any particular area (i.e. implementations or specific departmental functions)

03

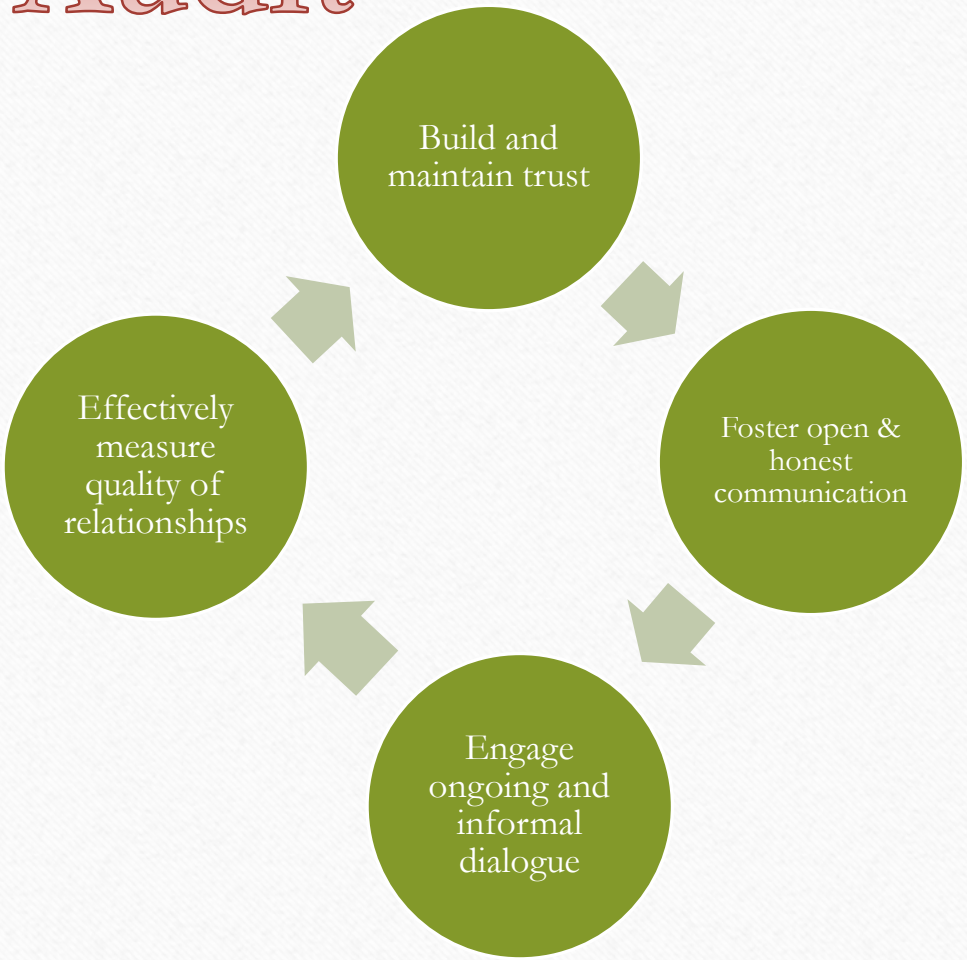
Discuss with Senior Leaders/Executive Management

										Full Audit			Limited Audit												
Current Risk Assessment				Year of Recent Reviews			Proposed Staff Hours Current Year			Proposed Schedule Current Year					Proposed Schedule Next Year					Proposed Schedule Two Years from				
#	Auditable Unit	Residual Risk	Priority	Three Years	Two Years	Last Year	Service Provider	IA	Total	Q1	Q2	Q3	Q4	Total Annual	Q1	Q2	Q3	Q4	Total Annual	Q1	Q2	Q3	Q4	Total Annual
1	Auditable Unit 6	4.50	High	✓		✓	15	20	35	20	15					5	15							
2	Auditable Unit 3	4.40	High	✓			20	20	40	20	20												25	
3	Auditable Unit 7	4.20	High		✓		20	20	40		20	20			15	5								
4	Auditable Unit 5	3.10	Medium	✓		✓		30	30			20	10									25		
5	Auditable Unit 11	3.00	Medium		✓											30	10							
6	Auditable Unit 8	2.80	Medium	✓	✓										5	10								
7	Auditable Unit 9	2.60	Medium	✓													15	15						
8	Auditable Unit 1	2.20	Medium	✓		✓										25	10							
9	Auditable Unit 2	2.10	Medium																	10	20			
10	Auditable Unit 4	1.20	Low		✓	✓																15	5	
11	Auditable Unit 10	1.00	Low		✓																	15	5	
	Effort Required in a Year						55	90	145	40	55	40	10	145	20	75	50	15	160	10	20	55	35	120
	Non Auditable Areas																							
1	Preparation for Audit & Risk Committee Meetings							30	30	9	7	7	7		9	7	7	7		9	7	7	7	
2	Updating Risk Assessment and Internal Audit Plan							50	50		15	15	20			15	15	20			15	15	20	
3	Consulting Assignments and Other Projects							15	15	10	5				10	5				10	5			
4	Follow-up Audits							80	80	20	20	20	20		20	20	20	20		20	20	20	20	
5	Staff Training							30	30	10	10	10			10	10	10			10	10	10		
6	Strategic Initiatives						20	45	65	20	20	0	25		10	10	10	10		10	10	10	10	
7	Carried forward audit engagements							10	10	10					10					10				
8	Quality Assurance							15	15				15					15					15	
	Total Effort Required						75	365	440	##	##	92	97	440	89	##	##	87	430	79	87	##	##	390

How to Engage Management and Executive Leaders

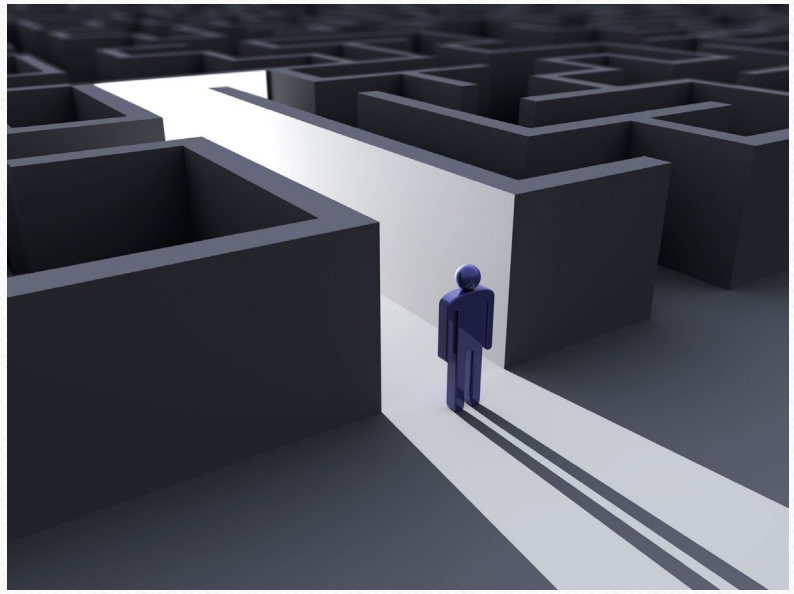
Key Tips

Critical to Audit



https://internalauditor.theiia.org/en/voices/2025/may/on-the-frontlines-stakeholder-relationships/

Challenges



- Loss of trust due to breakdown in communication
- Resistance or a lack of cooperation from the client or stakeholders
- Cultural misunderstandings or differences (e.g. professional behavior)
- Misalignment of how we perceive each other
- Language barriers

Ingredients for Success

- Who will be impacted?
- What are their interests, including needs and expectations?
- What are their concerns, including limiting factors and constraints?
- What is their level of power and influence?

Audience Type	Communication Style	Key Focus Areas	Technical Detail Level
Executive Leadership	Strategic and high-level	Business impact, resource needs, risk overview	Minimal technical jargon
Technical Teams	Detailed and precise	Technical requirements, control frameworks, testing procedures	High level of detail
Operations Staff	Practical and process-focused	Day-to-day impact, workflow changes, timeline	Moderate technical content
External Auditors	Professional and compliance-focused	Standards alignment, evidence requirements, control documentation	High technical precision

Video Break

How To...

Proposing the Plan and Soliciting Feedback

- Director/CAE discusses with administrative reporting line (if applicable and not the Audit Committee yet) and with senior management. May also include committees, if applicable.
- Meetings may be on an individual basis.
- Topics include risk assessment results, potential effects to the organization for those risks, how the results will aid the organization, and resource assignment.

Discussion:

What questions or concerns could management ask you and/or the CAE?

Possible Questions/Concerns:

- Have all risks and auditable units been considered?
- Are there any upcoming changes that have not been considered methodically, such as acquisitions, mergers, system upgrades, third-party suppliers, and software implementation?
- How do the plan's audit engagements link to the organization's objectives and top risks?
- How do the engagements add value for senior management and the organization?
- Do the coordination of assurance coverage and the schedule/timing of engagements make sense?
- If any requests have not been honored, why not?
- Does the plan include all engagements required by laws or regulations?

GIVE THEM THE OPPORTUNITY TO PROVIDE VALID FEEDBACK

Communicating to Finalize the Plan

- Usually presented to Audit Committee via a presentation.
- Be prepared for questions and possible feedback from management to the Audit Committee.
- Audit Committee may have questions and will either approve or ask for a revision.

Audit Plan

- ✓ Whatever methodology be sure to meet standards
- ✓ Consistent with Charter
- ✓ Right staff, adequate time
- ✓ Consider integration

Stakeholder Engagement

- ✓ Elicit input throughout planning and before finalizing plan
- ✓ Have reasoning for audits ready
- ✓ Maintain ongoing communications
- ✓ Evaluate communication/presentation options

Questions?

Lisa Siedzik

352-393-8875

siedzikl1@cityofgainesville.org

https://www.gainesvillefl.gov/Government-Pages/Government/City-Auditor

Linked In: Lisa Siedzik