

Risk Assessment
Audit Plan (Macro Level)
Engagement Planning (Micro Level)

Module Objectives



IDENTIFY PERTINENT IIA
STANDARDS



DISCUSS THE ROLE OF
GOVERNANCE, RISK AND
CONTROL FRAMEWORKS



DISCUSS DIFFERENT TYPES
OF RISK ASSESSMENTS



REVIEW THE AUDIT PLAN
RISK ASSESSMENT PROCESS



DISCUSS OBJECTIVES OF THE
ENGAGEMENT RISK
ASSESSMENT

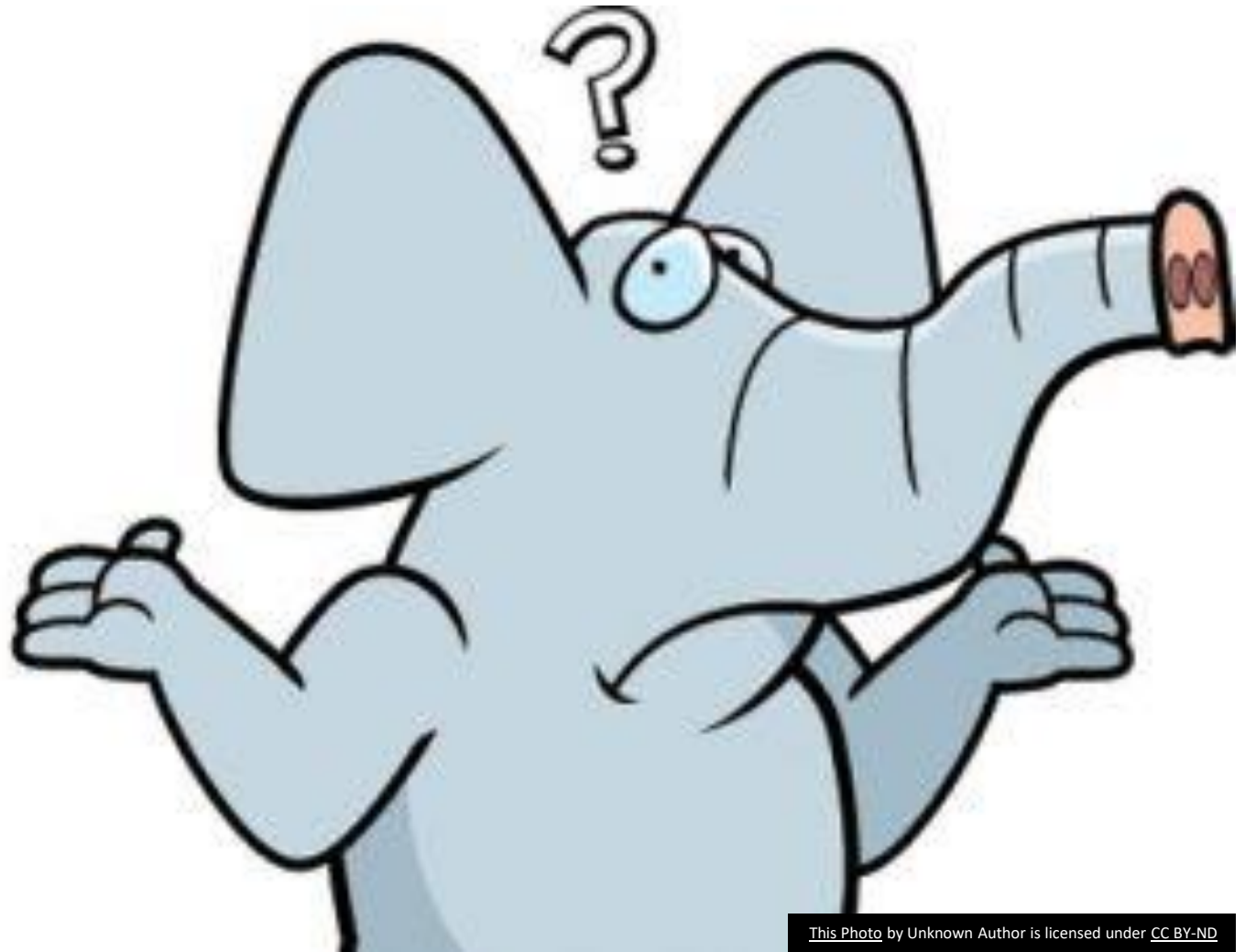


IDENTIFY RISK ASSESSMENT
TOOLS AND APPROACHES



DISCUSS EXAMPLES OF
ENGAGEMENT RISK
ASSESSMENT
METHODOLOGIES

Risk is a Confusing Term



This Photo by Unknown Author is licensed under [CC BY-ND](#)

“Risk Assessment”





The good old days





Each day we must strive for
CANI – Constant and
Never Ending Improvement

-Tony Robbins

Core Principles for the Professional Practice of Internal Auditing

- Demonstrates integrity.
- Demonstrates competence and due professional care.
- Is objective and free from undue influence (independent).
- Aligns with the strategies, objectives, and risks of the organization.
- Is appropriately positioned and adequately resourced.
- Demonstrates quality and continuous improvement.
- Communicates effectively.
- Provides risk-based assurance.
- Is insightful, proactive, and future-focused.
- Promotes organizational improvement.

Outline of the Competency Framework

- I. Professional Ethics: Promotes and applies professional ethics
- II. Internal audit management: Develops and manages the internal audit function.
- III. IPPF: Applies the International Professional Practice Framework.
- IV. Governance, risk and control: Applies a thorough understanding of governance, risk, and control appropriate to the organization.
- V. Business acumen: Maintains expertise of the business environment, industry practices, and specific organizational factors.
- VI. Communications: Communicates with impact
- VII. Persuasion and collaboration: Persuades and motivates others through collaboration and cooperation.
- VIII. Critical thinking: Applies process analysis, business intelligence, and problem solving techniques
- IX. Internal Audit delivery: Delivers internal audit engagements
- X. Improvement and innovation: Embraces change and drives improvement and innovation

Source: <https://na.theiia.org/about-us/Public%20Documents/The%20IIA%20Global%20Internal%20Audit%20Competency%20Framework.pdf>

<https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Core-Principles-for-the-Professional-Practice-of-Internal-Auditing.aspx>



IPPF

		Staff	Manager	CAE	Self Assessment Score	Areas for Improvement
1	Maintains current knowledge of the IPPF	x	x	x		
2	Leads the implementation of the IPPF in the internal audit function			x		
3	Demonstrates appropriate use and interpretation of the IPPF, seeking consultation if applicability is unclear	x	x			
4	Adheres to the requirements of the IPPF when planning and conducting an internal	x	x			
5	Adopts a risk based approach in accordance with The IPPF for annual audit plan, makes adjustments when needed		x	x		
6	Ensures internal audit has access to all systems, processes and people			x		
7	Exemplifies and monitors due professional care when conducting audit assignments	x	x			
8	Exemplifies and monitors due professional care of the internal audit team			x		
9	Leads on the development, implementation and review of the internal audit charter and receives approval from the board			x		
10	Ensures the independence of the audit function			x		
11	Establishes and maintains a quality assurance and improvement program			x		
12	Manages and supports a quality assurance and improvement program		x			
13	Discloses non conformance with the Code of Ethics and International Standards for Professional Practice of Internal Audit with senior management and board			x		

Governance, Risk & Control

		Staff	Manager	CAE	Self Assessment Score	Areas for Improvement
1	Educates senior management and board on best practices in governance, risk and			x		
2	Evaluates the appropriateness of the organization's frameworks for governance, risk		x	x		
3	Contributes to the development of risk oriented culture within the organization			x		
4	Maintains a comprehensive insight into the organization's current and emerging risk			x		
5	Monitors future risk changes to the organization based on political, economical, social, environmental, legal or technological factors and their potential impact			x		
6	Operates within the organization's frameworks for governance, risk and control	x	x	x		
7	Creates audit engagement plans based on the risk and its impact on the organization	x	x			
8	Applies the concepts of controls during audit activities	x	x			
9	Assesses IT governance		x	x		
10	Ensures internal audit activities are aligned with and enhances the organization's enterprise risk management strategy and risk profile		x	x		
11	Ensures that proposals for improvements to internal controls are balanced with organizational objectives and capabilities		x			
12	Provides an explanation on the risk profile of the organization to board and senior			x		
13	Provides an explanation on the risk profile of the internal audit engagement to	x	x			
14	Supports a culture of fraud risk awareness at all levels of the organization	x	x	x		
15	Assesses and accounts for the potential for fraud risk and identifies common types of fraud associated with the organization		x	x		
16	Assesses and accounts for the potential for fraud risk and identifies common types of fraud associated with the internal audit engagement	x	x			
17	Maintains an understanding of the processes used to support fraud investigations	x	x	x		

Internal Audit Management						
		Staff	Manager	CAE	Self Assessment Score	Areas for Improvement
1	Advocates the internal audit function and its value throughout the organization			X		
2	Acts as a role model by exemplifying high performance for team members		X	X		
3	Analyzes own strengths and weaknesses to maximize personal contribution to the organization	X	X	X		
4	Anticipates and responds sensitively to staff problems, concerns and questions		X	X		
5	Articulates clear expectations and business goals and links these to organizational strategy		X	X		
6	Sets clear performance standards for internal auditors and the internal audit function			X		
7	Strives for quality and excellence and encourages others to do the same	X	X	X		
8	Delegates tasks in a constructive and supportive fashion		X	X		
9	Takes personal accountability for results delivered in areas of responsibility	X	X	X		
10	Monitors staff performance and workload and provides constructive and timely feedback to help others achieve their goals		X	X		
11	Coaches others to enhance their competence and professional development		X	X		
12	Develops and implements a plan for professional development for members of the internal audit function		X	X		
13	Continues professional development and utilizes relevant learning opportunities	X	X	X		
14	Provides opportunities and proactive input in the development and career needs of others		X	X		
15	Assesses self-development and career needs and takes advantage of new challenges as opportunities for personal and professional growth	X	X	X		
16	Maintains up-to-date competencies required for effective internal audit delivery	X	X	X		
17	Adjusts the internal audit team skill mix and diversity according to organization's objectives and risks			X		
18	Establishes recruitment systems that consistently result in competent performers being hired			X		
19	Uses a variety of assessment tools and tests to assess a candidate's capability and competence			X		
20	Supports and contributes to the recruitment process within the internal audit function	X	X			
21	Maintains a regularly updated succession planning strategy			X		
22	Values and promotes diverse viewpoints and cultural sensitivity	X	X	X		
23	Applies a knowledge of human resource processes and leadership styles to supporting and directing others	X	X	X		

Business Acumen

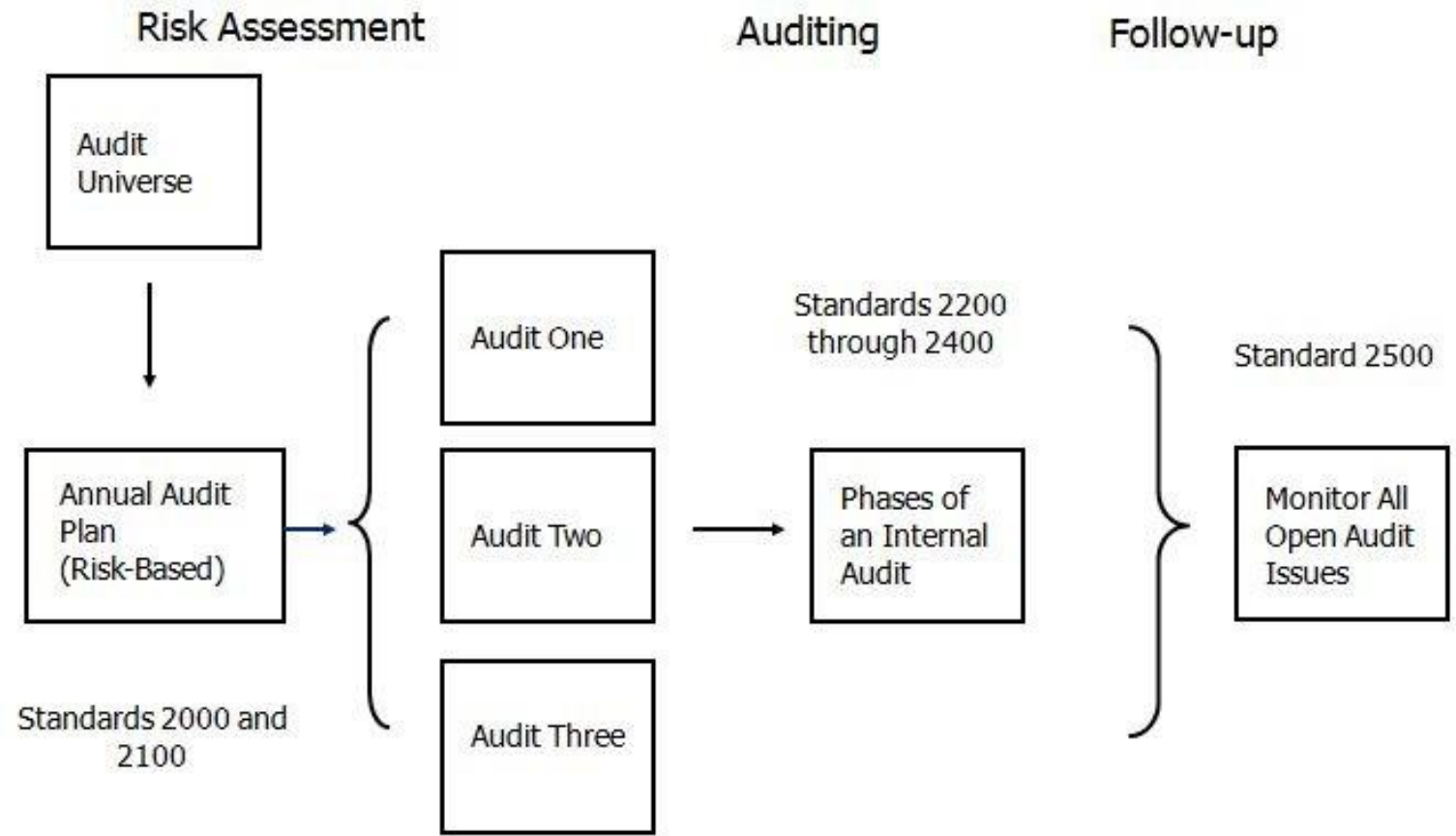
		Staff	Manager	CAE	Self Assessment Score	Areas for Improvement
1	Maintains knowledge of the organization and its risks		X	X		
2	Maintains industry specific knowledge appropriate to the audit engagements	X				
3	Maintains industry specific knowledge appropriate to the organization		X	X		
4	Assesses and takes account of basic macroeconomic and microeconomic factors and relevance to the audit engagements	X				
5	Assesses and takes account of macroeconomic and microeconomic factors and the impact on the organization		X	X		
6	Maintains a current understanding of the latest global developments, regulatory and legal requirements and assesses the relevance to the audit engagements	X				
7	Maintains a current understanding of the latest global developments and regulatory and legal framework within which the organization operates		X	X		
8	Maintains knowledge of the technical aspects of financial, managerial and cost accounting concepts, standards, systems and reporting processes appropriate to the	X				
9	Assesses and takes account of the technical aspects of financial, managerial and cost accounting concepts, standards, systems and reporting processes appropriate to the		X	X		
10	Assesses and takes account of how IT contributes to organizational objectives, risks associated with IT, and relevance to the audit engagements	X	X			
11	Demonstrates sound working knowledge of the quality control frameworks relevant to the audit engagements	X	X			
12	Evaluates the quality control frameworks operated by the organization			X		
13	Takes account of cultural aspects of the organization	X	X	X		
14	Takes account of the mission, strategic objectives and business nature of the	X	X	X		

Internal Audit Delivery						
		Staff	Manager	CAE	Self Assessment Score	Areas for Improvement
1	Applies the organization's audit methodology and carries out the audit procedures to meet the specific audit engagement objectives	x	x			
2	Ensures the quality of planning and delivery of audit engagements			x		
3	Supervises the execution of audit engagements to ensure that objectives are met and		x			
4	Maintains objectivity throughout the audit engagements	x	x	x		
5	Manages all resources efficiently to ensure the engagement objectives are met	x	x			
6	Demonstrates efficiency and persistence, managing own time and ensuring engagement deadlines and objectives are met	x				
7	Develops, implements and monitors project plans to ensure delivery in accordance with agreed timelines		x			
8	Selects and applies the appropriate tools and techniques to data gathering, analysis and interpretation, and reporting.	x	x			
9	Plans and conducts audit engagements to identify key risks and controls	x	x			
10	Identifies resources needed and addresses limitations for audit engagement			x		
11	Obtains reliable, relevant and sufficient evidence and evaluates critically	x	x			
12	Identifies and escalates the strategic implications to the organization from audit			x		
13	Develops and ensures that working papers are a true reflection of all activities performed during the audit engagement	x				
14	Presents findings and proposes recommendations that deal with root cause of issues and impact to the organization	x	x			
15	Provides assurance and advisory services to senior management and the board		x	x		
16	Ensures that the scope of work is appropriate for the audit assignment		x			
17	Establishes a follow-up process to monitor management actions			x		
18	Follows up with management to ensure that management actions have been effectively implemented or that senior management has accepted the risk of not	x	x			

Improvement and Innovation

	Staff	Manager	CAE	Self Assessment Score	Areas for Improvement
1 Champions change, continuous improvement and innovation and supports others in the pursuit of these			x		
2 Seeks and justifies opportunities for continuous improvement	x	x			
3 Initiates and manages change within sphere of responsibility	x	x	x		
4 Encourages others to embrace change by explaining the intended benefits	x	x	x		
5 Provides a vision for how change is implemented in the organization			x		
6 Encourages others to propose innovative ideas and provides positive feedback to ensure new ideas are progressed		x	x		
7 Contributes to insight and proposals for change and improvement		x	x		
8 Makes a significant contribution to organizational change strategy			x		
9 Investigates and analyzes the reasons for change in the organization		x	x		
10 Identifies the risks associated with change and adapts audit activity to manage the risks	x	x	x		
11 Assesses the potential barriers and resources for change initiatives	x	x	x		
12 Implements change programs across the audit function and team		x	x		
13 Maintains personal performance and effectiveness in changing and ambiguous	x	x	x		
14 Accommodates new priorities and implements positive changes in area of work	x	x	x		
15 Adjusts team priorities to new and changing priorities of the organization		x	x		
16 Anticipates reactions to change and adapts own style to support others	x	x	x		

Risk-Based Auditing

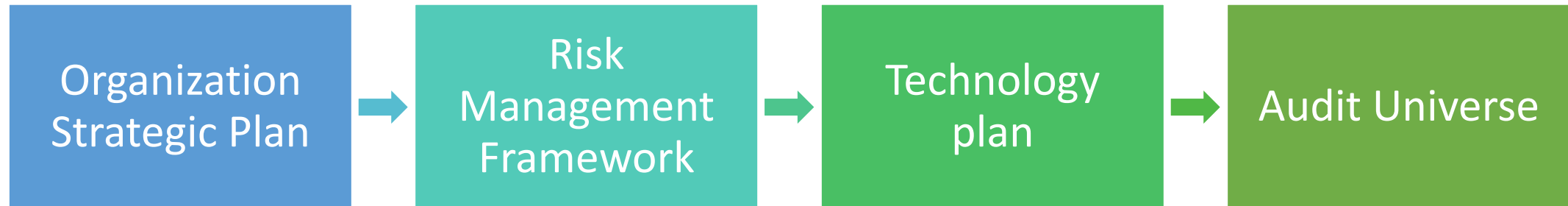


Macro-level, or Entity- wide, Risk Assessment

2010 – Planning - The chief audit executive must establish risk-based plans 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.

Risk Based Audit Plan



Risk Assessment – Audit Universe

One of the first steps in developing annual audit plans is to define the total universe of auditable units. The audit universe is the sum of all auditable units. Auditable units are those parts of the organization that are exposed to sufficient risks such that control, including audit, is appropriate. Not every activity or every asset of an organization requires the attention of internal auditing. In order to become an "auditable unit," the unit must:



1. Contribute to the organization's goals.



2. Be sufficiently large as to have a noticeable impact on the organization (also known as materiality or significance or business impact).



3. Be sufficiently important to justify the cost of control, so that the potential loss should be greater than the expense of control, including the expense of audit.

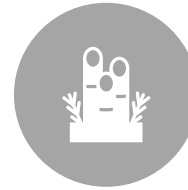
Risk Assessment – Audit Universe

Once you have identified all the entities in the Audit Universe, make sure that they are all covered in a multiple year plan or that you document why an area is not covered. Some low risk areas may not be covered every year but you will be able to see coverage over the course of multiple years. This has been an issue with some QAR and with some banking regulators.

Risk Assessment – Auditable Units



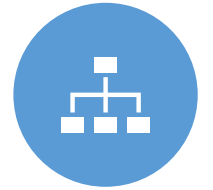
AUDITABLE UNITS CAN
BE OF NUMEROUS
TYPES:



LOCATIONS: BRANCHES,
DIVISIONS, PLANTS,
OFFICES, ETC.



PROJECTS: SYSTEMS,
PROGRAMS,
APPLICATIONS,
PRODUCTS, ETC.



ACTIVITIES: BUSINESS
UNITS, FUNCTIONS,
PROCESSES, ETC.



ASSETS: PHYSICAL,
ACCOUNTS, CASH,
INFORMATION,
RESOURCES, ETC.



ANY COMBINATION OF
THE ABOVE.



DON'T OVER
COMPLICATE IT!

Risk Assessment Model Sample

An internal audit risk model is used to quantify the risk rating of each audit unit. Internal audits are then scheduled by risk priority. Within each audit unit, a micro risk assessment is performed to determine specific testing that should be performed in each area to ensure higher risk areas have appropriate coverage. The Macro Risk Assessment which is a high level risk assessment is based on factors or elements of risk. Samples of these factors are noted below.

- Dollar or Transaction Volume
- Quality of Internal Controls
- Complexity
- Technology Impact
- Prior Audit Findings
- Management Changes
- Regulatory Impact
- Rapidity of Growth

Risk Assessment Model Sample

- Other factors to consider are as follows:
- Review by External Auditors, compliance, loan review, branch assessments etc.
- Coverage in SOX Testing, ARMICS, ERM etc.

Audit Plan based on Risk Assessment

Internal audit plan is prepared based on audit universe, input from Senior Management and the BOD and an Annual Risk assessment.

The plan must be reviewed and updated periodically (perhaps quarterly) throughout the year to reflect changes in the organization's:

- Business
- Operations
- Programs
- Systems
- Controls



Performance Standards – 2010.A2 Planning

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.



Performance Standards – 2010.C1 Planning

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.

Micro-level,
or Activity-
based, Risk
Assessment

2200 Engagement Planning
- Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations.

Micro-level, or Activity- based, Risk Assessment

2201 Planning Considerations - In planning the engagement, internal auditors must consider:

The objectives of the activity being reviewed and the means by which the activity controls its performance;

The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level;

The adequacy and effectiveness of the activity's risk management and control processes compared to a relevant control framework or model; and

The opportunities for making significant improvements to the activity's risk management and control processes.

Micro-level, or Activity- based, Risk Assessment

2210 Engagement Objectives - Objectives must be established for each engagement.

2210.A1 Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

2210.A2 Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

2210.A3 Adequate criteria are needed to evaluate controls. Internal auditors must ascertain the extent to which management has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must work with management to develop appropriate evaluation criteria.

Standards Requirements for Assurance and Consulting Engagements

Assurance	Consulting
<p>When planning an engagement for parties outside the organization, internal auditors must establish a written understanding with them about the objectives, scope, and other expectations (Standard 2201.A1).</p>	<p>Internal auditors and consulting engagement clients must agree on engagement objectives, scope, expectations, and responsibilities and must document this if the engagement is significant (Standard 2201.C1).</p>
<p>The objectives of assurance engagements must be aligned with the results of a preliminary assessment of the risks relevant to the area or process under review (Standard 2210.A1).</p>	<p>Objectives must address governance, risk management, and control processes to the extent agreed upon with the client (Standard 2210.C1).</p>
<p>When developing engagement objectives, internal auditors must consider the probability (often referred to as likelihood) of significant errors, fraud, noncompliance, and other exposures (Standard 2210.A2).</p>	<p>Engagement objectives must be consistent with the organization's values, strategies, and objectives (Standard 2210.C2).</p>
<p>Internal auditors must identify adequate and appropriate criteria by which to evaluate whether relevant objectives and goals have been accomplished (Standard 2210.A3).</p>	<p>Throughout the engagement, internal auditors must address controls consistent with the engagement objectives and be alert to significant control issues (Standard 2220.C2).</p>

Engagement Planning Steps



- ✓ Understand Context
- ✓ Gather Information
- ✓ Assess Risks
- Form Objectives
- Establish Scope
- Allocate Resources
- Document Plan

Engagement Planning Steps



- ✓ Understand Context
- Gather Information
- Assess Risks
- Form Objectives
- Establish Scope
- Allocate Resources
- Document Plan

Engagement Planning Steps



- ✓ Understand Context
- ✓ Gather Information
- Assess Risks
- Form Objectives
- Establish Scope
- Allocate Resources
- Document Plan

Phase 1 - Obtain an understanding of the audit area – Audit area and Report Users



Review P&P



Review Organizational Charts



Review any Organizational Risk Assessments (including risk)



Arrange Kick-off meetings



Perform Walkthroughs



Review previous internal, external and regulatory reports



Determine Information Systems used by audit area



Determine any legal or regulatory requirements

Engagement Planning Steps



- ✓ Understand Context
- ✓ Gather Information
- ✓ Assess Risks
- Form Objectives
- Establish Scope
- Allocate Resources
- Document Plan

Identify Inherent Risks



Anything that prevents an objective from being achieved.



What could go wrong?



What keeps you up at night?

Sample Risk/Control Matrix

Objectives	Inherent Risks	Impact/ Likelihood	Controls (and other Risk Management Techniques)	Evaluation of Adequacy	Tests of Effectiveness	Final Evaluation

Example

Business Objective	Inherent Risk	Impact (L,M,H)	Likelihood (L,M,H)	Control
A. Personnel expenses are appropriate and authorized.	A.1 Corporate cards are issued inappropriately, resulting in fraudulent expenses.	M	M	Duties are segregated.
	A.2 Personnel are not provided guidance on corporate card usage and expense policies, resulting in inappropriate expenses.	L	M	Expense policy is communicated to personnel authorized to incur organizational expenses.
	A.3 Expense reports are not submitted/reviewed timely, resulting in inappropriate expenses.	H	H	No control is in place.
	A.4 Expense reports with receipts are not reviewed and approved by appropriate personnel, resulting in inappropriate expenses.	H	M	Approvals are based on management hierarchy. Expense reports cannot be submitted until a manager approves them. Expense team conducts monthly reviews.
B. Operating expenses are appropriate and authorized.	B.1 Fictitious vendors are set up in the system, resulting in fraudulent expenses.	H	L	Duties are segregated.
	B.2 Vendors submit inaccurate, duplicate, or fictitious invoices that are not reviewed and approved by appropriate personnel.	H	M	Invoice approval is based on expense authorization limits.
	B.3 Expenses are not approved before committed to, resulting in inappropriate expenses.	M	L	No control is in place.
C. Payments are accurate and timely.	C.1 Payments are made after the due date, resulting in interest and penalties.	L	M	No control is in place.
	C.2 Discounts are not realized due to payments made after the discount date.	L	H	No control is in place.

Assess Risk Impact and Likelihood



Impact of the risk event if it occurs



How likely is it that the risk event will occur?

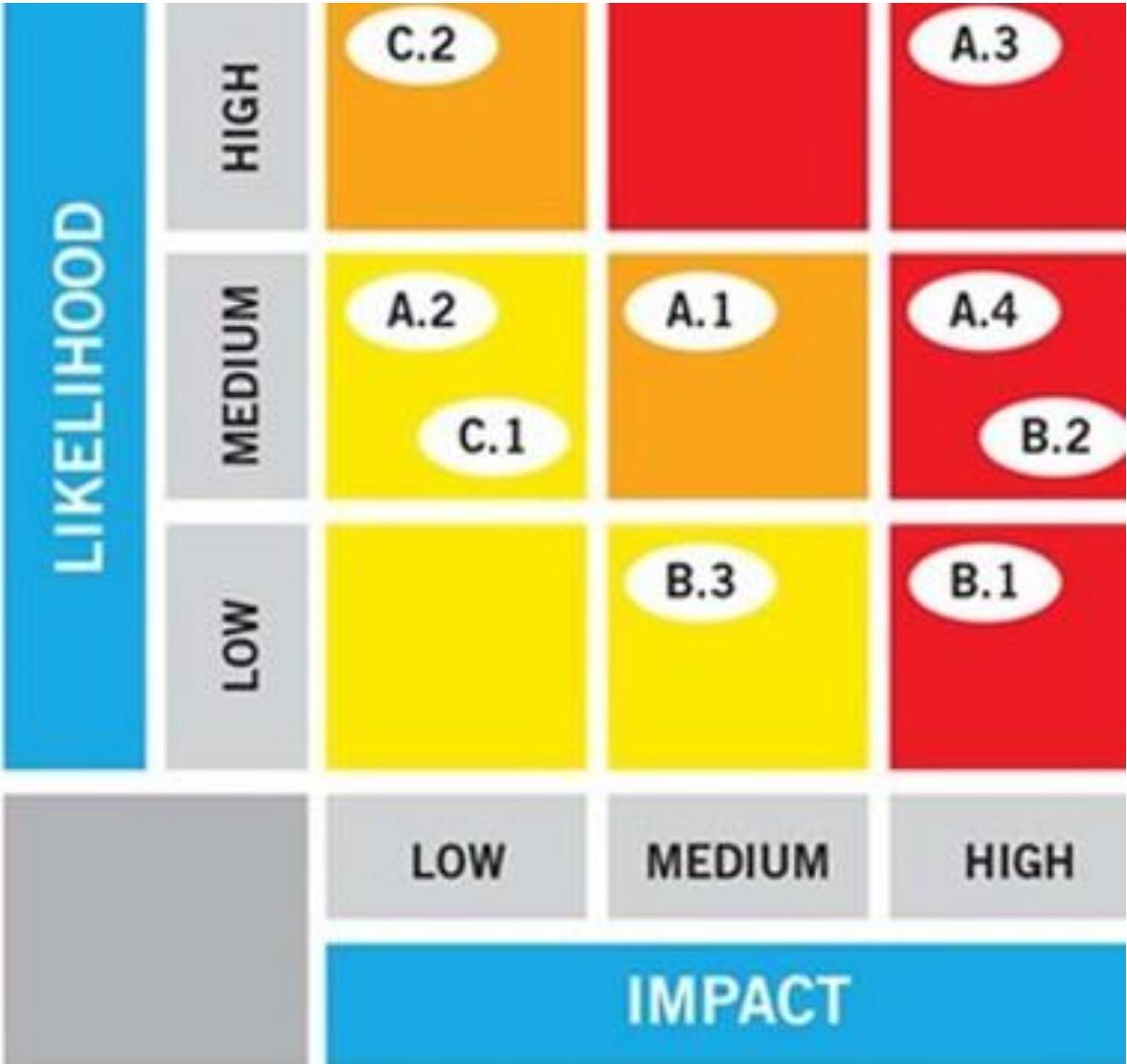


Typically assessed as high, medium or low

Example

Business Objective	Inherent Risk	Impact (L,M,H)	Likelihood (L,M,H)	Control
A. Personnel expenses are appropriate and authorized.	A.1 Corporate cards are issued inappropriately, resulting in fraudulent expenses.	M	M	Duties are segregated.
	A.2 Personnel are not provided guidance on corporate card usage and expense policies, resulting in inappropriate expenses.	L	M	Expense policy is communicated to personnel authorized to incur organizational expenses.
	A.3 Expense reports are not submitted/reviewed timely, resulting in inappropriate expenses.	H	H	No control is in place.
	A.4 Expense reports with receipts are not reviewed and approved by appropriate personnel, resulting in inappropriate expenses.	H	M	Approvals are based on management hierarchy. Expense reports cannot be submitted until a manager approves them. Expense team conducts monthly reviews.
B. Operating expenses are appropriate and authorized.	B.1 Fictitious vendors are set up in the system, resulting in fraudulent expenses.	H	L	Duties are segregated.
	B.2 Vendors submit inaccurate, duplicate, or fictitious invoices that are not reviewed and approved by appropriate personnel.	H	M	Invoice approval is based on expense authorization limits.
	B.3 Expenses are not approved before committed to, resulting in inappropriate expenses.	M	L	No control is in place.
C. Payments are accurate and timely.	C.1 Payments are made after the due date, resulting in interest and penalties.	L	M	No control is in place.
	C.2 Discounts are not realized due to payments made after the discount date.	L	H	No control is in place.

Heat Map



Significant Risks

Inherent Risk	Impact (L,M,H)	Likelihood (L,M,H)
A.3 Expense reports are not submitted/reviewed timely, resulting in inappropriate expenses.	H	H
A.4 Expense reports with receipts are not reviewed and approved by appropriate personnel, resulting in inappropriate expenses.	H	M
B.2 Vendors submit inaccurate, duplicate, or fictitious invoices that are not reviewed and approved by appropriate personnel.	H	M
B.1 Fictitious vendors are set up in the system, resulting in fraudulent expenses.	H	L
A.1 Corporate cards are issued inappropriately, resulting in fraudulent expenses.	M	M
C.2 Discounts are not realized due to payments made after the discount date.	L	H

Risk Responses

Avoidance

Reduction

Sharing

Acceptance

Identify Criteria



POLICIES &
PROCEDURES



LAWS &
REGULATIONS



TECHNICAL
STANDARDS



PERFORMANCE
BENCHMARKS



IT STANDARDS
(E.G. NIST)

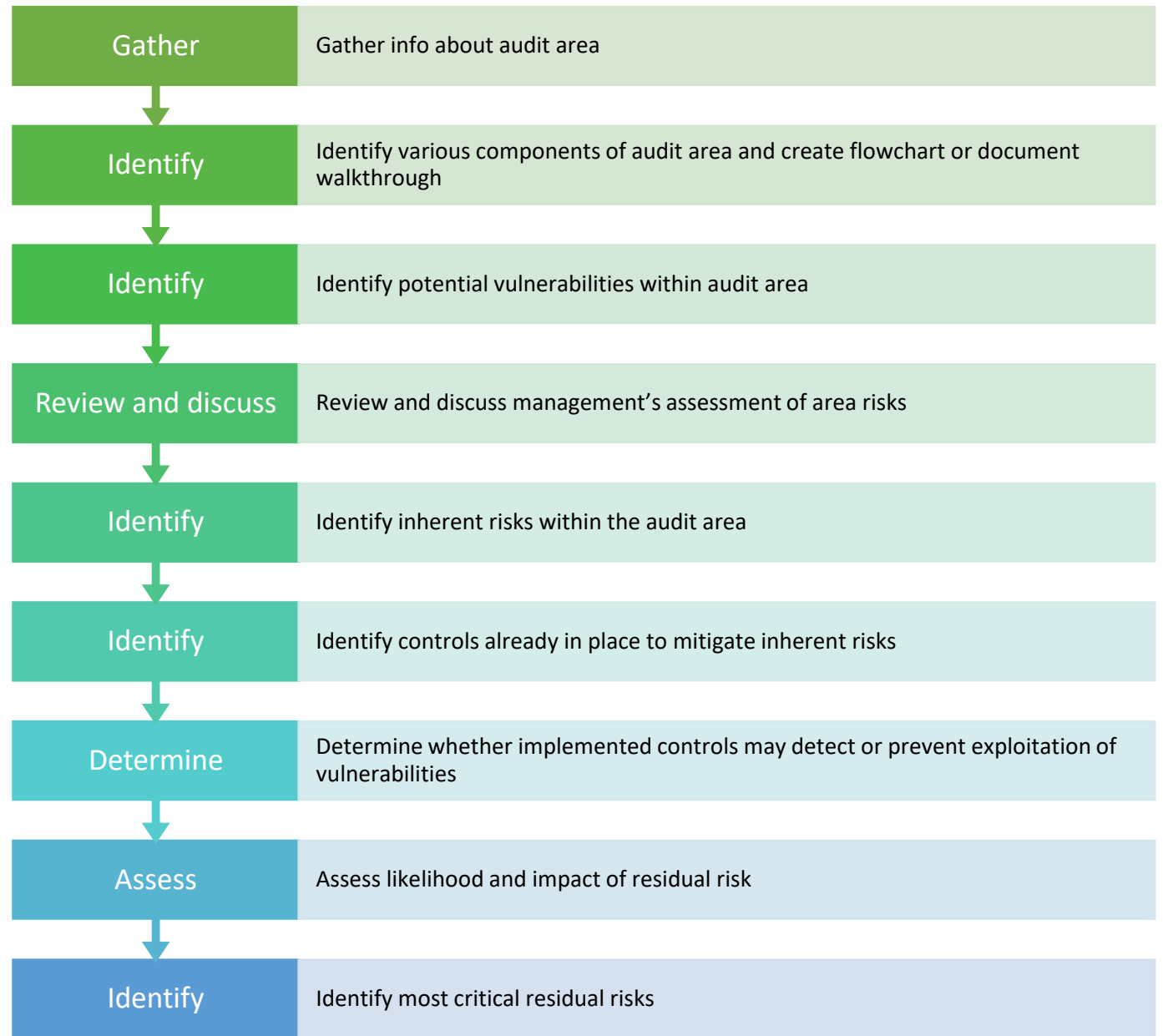


FASB, GASB,
GAGAS



IPPF

Perform Engagement Risk Assessment



Audit Objectives, Scope & Methodology

Use risk assessment to define clear audit objectives

Objectives should be geared towards greatest risk

Define Scope related to Timing prior to start of audit

Determine whether the audit team will:

- Test controls only
- Perform substantive testing where controls are missing or subpar
- Extent of procedures (e.g. sample size)

Methodologies

- Sampling
- Interviews/questionnaires
- Observations
- Walkthroughs

Engagement Planning Steps



- ✓ Understand Context
- ✓ Gather Information
- ✓ Assess Risks
- Form Objectives
- Establish Scope
- Allocate Resources
- Document Plan

Current Trends

“Don’t Manage Risk – Manage Value”

Marinus de Pooter
July 11, 2019



<https://iaonline.theiia.org/>

Questions?

Michelle Fowler, CPA, CIA, CISA, CRMA

Founder and President

mfowler@fowlerandcompany.com

804-350-8654

www.fowlerandcompany.com

<https://internalauditcareeracademy.com/>