A chance to reframe Internal Audit: the new Global Internal Audit Standards*

Risk Assessment and IA Plan Coverage

Global Internal Audit Standards: 9.4 Internal Audit Plan

What it is

IA's ability to deliver relevant and impactful services to the organisation is dependent upon a well-executed Risk Assessment and thoughtfully-designed IA Plan.

What's new in the requirements?
The new Standards now include requirements for IA to communicate to senior management and the Board:

- Any high risk areas where an assurance engagement is not included on the IA Plan
- Conflicting demands for services between major stakeholders such as those driven by high priority or emerging risks
- Impact of resource limitations on IA coverage

IA must also demonstrate that it considered coverage of Information Technology (IT) governance, fraud risk, the effectiveness of the compliance and ethics programs, in addition to other high-risk areas.

Am I required to document a thorough audit universe and formally calculate IA's coverage?
These elements remain considerations and are not explicitly required in the Standards. There is, however, an implication that IA understands the risk universe and can form a view on what to include in the Plan. This could be accomplished through a basic mapping of IA's Plan against the universe of ERM defined risks, showing which are covered and which are not. If you do elect for a more detailed auditable entity universe, make sure you include those emerging and horizontal (e.g., process, enterprise) risk topics that don't always fit neatly into a known, single entity component.

The opportunity to advance IA

Unlocking benefits beyond the Standards

Listening to stakeholder concerns is important, but translating them into targeted projects to address the organisation's specific needs is crucial. IA teams that can design projects that appropriately serve the organisation provide a great value. Here are tips to do that:

Risk Assessments should be data-informed
One of the efficient ways to identify risk is to monitor risk indicators periodically through data. This is also an effective way to expand IA's coverage efficiently and maintain on an up to date understanding of select risk drivers and pivot IA's effort when needed.

IT and cyber risks require a targeted, deeper dive Risk Assessment
IT and cyber risks are too complex and multi-faceted to be sufficiently captured within typical high-level Risk Assessment procedures. In order for IA to be able to demonstrate that IT or cyber engagements on its Plan are based on an understanding of risk drivers, a more detailed Risk Assessment is necessary in addition to obtaining any separate risk assessments that IT performed. Often this leads to the development of a multi-year Plan that can continuously evolve.

Engagement level Risk Assessments are required
The new Standards require an engagement Risk Assessment to demonstrate IA's understanding of the specific risk drivers within an activity under review. This requires a stronger linkage from the overall Risk Assessment process to engagement-level planning.

*Global Internal Audit Standards ("Standards") is a registered trademark of The Institute of Internal Auditors, Inc. ("IIA").

Where to Start

The checklist below includes both common and leading Risk Assessment practices for you to use to evaluate the maturity of your existing process and consider opportunities for enhancements.

Gather

❑ Obtain the latest **organisation strategy** and organisational data, including executive's performance objectives.

❑ Obtain **risk assessments performed by other functions** (e.g., 10-K, Corporate compliance, CISO, SOX, Quality).

❑ Obtain additional direct data input from other risk, assurance, and compliance **monitoring activities including testing results**, whistleblower hotline and other ethics matters / trends, and prior IA Plan results.

❑ Obtain input from **external sources** including industry publications and direct competitors.

❑ Obtain direct input from **stakeholders** (including the Board and senior management) from a wide representation across the organisation. Use the information obtained in the previous steps to prepare for these interviews and make your lines of inquiry more targeted.

❑ Consider **coordinating** and conducting risk interviews with other risk and assurance providers (e.g., ERM team, Compliance) to minimise disruption to stakeholders on similar topics.

❑ Consider the need to bring **specialists** to risk interviews over more technical and complex risk topics (e.g., climate, sustainability, cyber, data modeling) to drive a more robust discussion and yield greater insights.

❑ Consider use of more advanced tools such as **AI** for prompts to perform research on key risks, develop draft interview questions, analyse and document results of interviews, and to suggest IA focus areas.

Assess

❑ Formally link IA's Risk Assessment to the **ERM risk taxonomy**. When IA is the facilitator of ERM or directly leverages ERM's Risk Assessment, it's important to document how those results informed IA's specific Plan.

❑ Leverage **key risk indicators (KRIs)** within the Risk Assessment process for processes or risk areas with high quality data to inform IA's assessment. Analyse data for anomalies or new risk indicators.

❑ Analyse inputs and data sources to assess risk. **Visualise** the risk assessment results and highlight potential gaps and overlap in coverage.

❑ Layer in IA's understanding of **risk coverage** across the organisation and how that was used to inform IA's proposed Plan (Refer to our issue #5 "Assurance Ecosystem").

❑ Assess where IA could add value (e.g., highest risk, regulatory requirement, significant strategic priority linkage), and which type of engagement (e.g., assurance, advisory) is most relevant to draft the **initial IA Plan**.

❑ Reference IA's **backlog** of potential projects to the current Risk Assessment results.

❑ **Visualise** IA's proposed Plan across multiple dimensions as a means to demonstrate both risk linkage and coverage - ERM risk linkage, organisation strategy linkage, divisional linkage, risk type. Reflect on IA's balance of core or foundational processes/audit universe based projects verse event-based or emerging risk areas (i.e., business model reinvention, emerging regulations, technology transformation, etc.)

❑ Identify the **resources** (financial, people and technology) needed to execute the proposed Plan to confirm with senior management and the Board.

Socialise

❑ Share IA's proposed Plan with other **risk, assurance and compliance functions** and consider adjustments as needed based on feedback received.

❑ Socialise IA's proposed Plan with **senior management** and consider adjustments as needed based on feedback received.

❑ Visually **present** both the results of the Risk Assessment and the proposed IA Plan to the Board including the required communications per the Standards and obtain formal approval.

Continuously Monitor & Adjust

How it Comes Together

To develop a strong IA Plan, IA needs to take into account various considerations and interdependencies within the IA framework. Those interdependencies are represented below as shaded building blocks that tangentially impact or are impacted by the Risk Assessment and IA Plan and should be considered together.

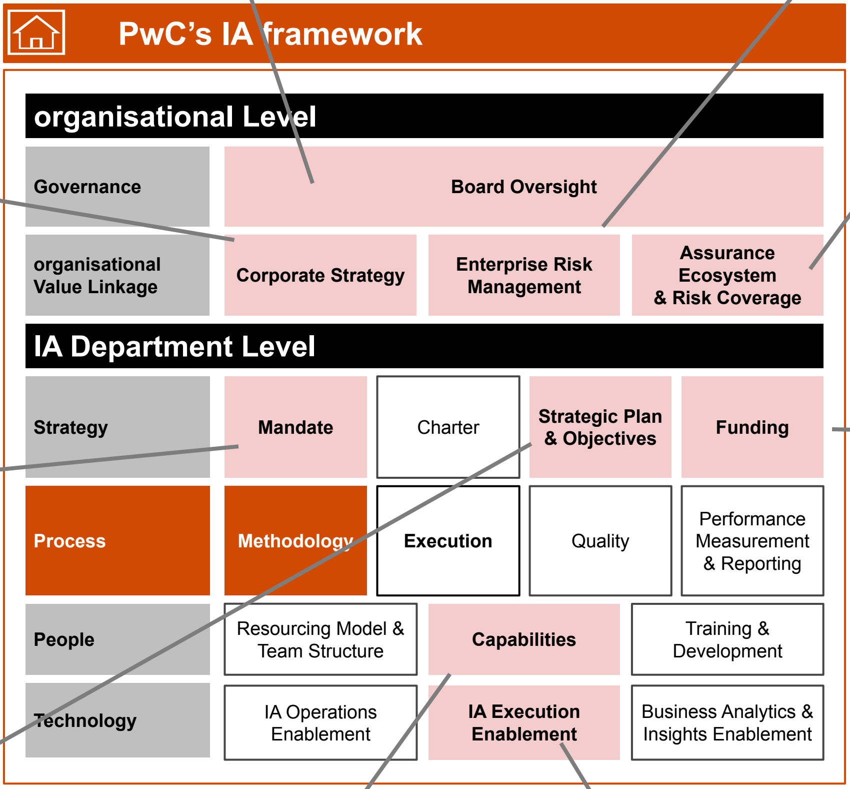
Questions and interdependencies for consideration

How well does the IA Plan link to relevant risks facing the organisation? Is IA addressing all risks considered high within its Plan?

What coverage of ERM risks are included in IA's Plan?

How explicit is the linkage of IA's Plan to the organisation's strategy?

How has IA considered the work of other internal assurance providers in its Plan development?



PwC's IA framework

organisational Level				
Governance	Board Oversight			
organisational Value Linkage	Corporate Strategy	Enterprise Risk Management	Assurance Ecosystem & Risk Coverage	
IA Department Level				
Strategy	Mandate	Charter	Strategic Plan & Objectives	Funding
Process	Methodology	Execution	Quality	Performance Measurement & Reporting
People	Resourcing Model & Team Structure	Capabilities	Training & Development	
Technology	IA Operations Enablement	IA Execution Enablement	Business Analytics & Insights Enablement	

Does the IA Plan align with what was set out in the mandate?

Now that IA has its Plan for the year, what resources and investments are needed? For example, technology, co-source providers, upskilling etc.

Has IA's Risk Assessment approach and Plan further enforced the strategic vision it has set out to accomplish?

Does IA have the capabilities to execute on the IA Plan?

Has IA utilised analytics to monitor KRIs as an input into their Risk Assessment and hone in on elevated risk in the organisation? Are KRIs monitored and adjustments made to the Plan periodically?

🟥 Article topic ▨ Direct interdependency

*Global Internal Audit Standards ("Standards") is a registered trademark of The Institute of Internal Auditors, Inc. ("IIA").

The stakeholder perspective

As leaders sitting outside of IA, you play an important role in discussing the top risks facing the organisation and confirming those risks get sufficient coverage through IA's Plan. When discussing IA's Risk Assessment and Audit Plan, consider the following:

Board/Audit Committee & Senior Management

How well do the Risk Assessment results and IA plan reflect the Board and senior management's perspective of the top risks to the organisation including consideration of key strategic initiatives?

Do you have a clear view on how the organisation is mitigating those top risks across the various operating lines and how that view is driving IA's proposed Plan?

To what extent does IA leverage data and KRIs in the Risk Assessment process?

How well do you understand how IA's proposed projects link to the results of the Risk Assessment?

Do you understand how resourcing (financial, human and technological) limitations impact IA's Plan?

Is the mix of types of risks covered within IA's Plan (i.e. financial, IT, operational, compliance, fraud, strategic) in line with their mandate and where you desire them to focus effort?

Second Line (e.g., Risk, Compliance)

Do you have sufficient transparency into IA's Risk Assessment process and how it links to risk assessments performed within your function?

Does IA's Risk Assessment process and Plan consider an integrated assurance approach with second line, to maximise coverage and avoid duplication?

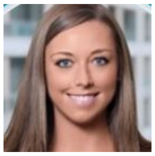
Are there opportunities to support IA with knowledge to enable their audits, whether from other second line functions or external support?

How well integrated and automated are the inputs and data that are shared across various risk assessments performed?

Contact us:

Andy Banks

Partner, PwC Ireland Internal Audit Lead
Andy.j.banks@pwc.com



Marian Barry

Director, Internal Audit
Marian.x.barry@pwc.com

Aoife Finnegan

Director, Internal Audit
Aoife.finnegan@pwc.com

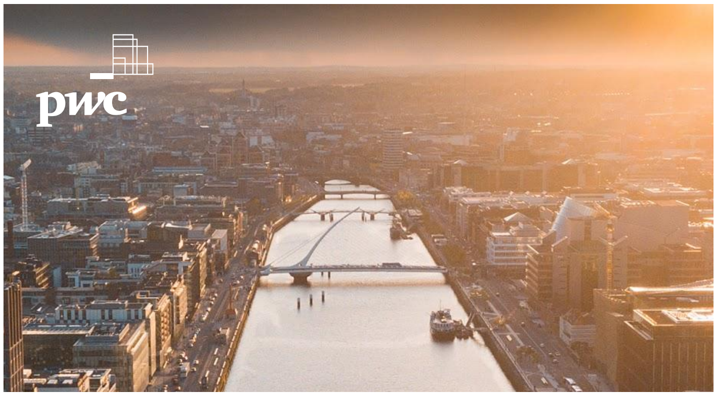
Fiona Leahy

Manager, Internal Audit
fiona.e.leahy@pwc.com

! Key Resources

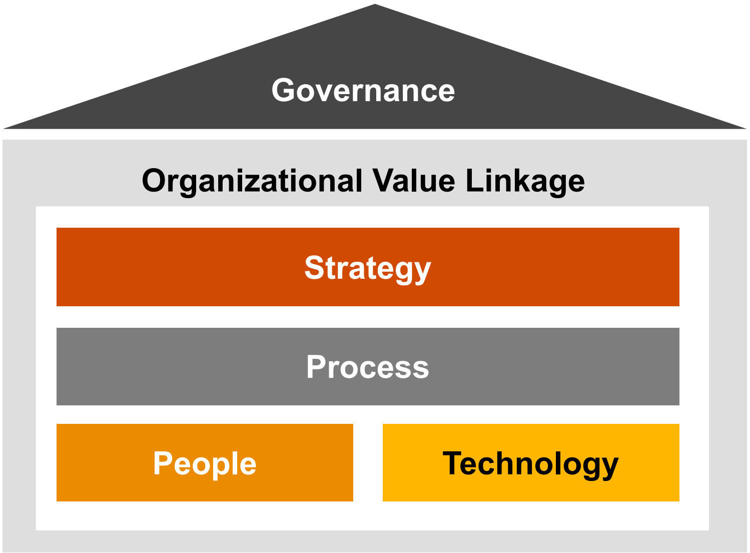
- Resources from the IIA:
  – Global Internal Audit Standards ™
- PwC Global Internal Audit Study 2023
- PwC Ireland Internal Audit Study 2023
- Governance Insights Center website

Certain links in this material connect to other Web Sites maintained by third parties over whom PwC has no control. PwC makes no representations as to the accuracy or any other aspect of information contained in other Web Sites.



Reframe IA Series

Practical ways to implement the IIA's new Global Internal Audit Standards and IA transformation.



Governance

Organizational Value Linkage

Strategy

Process

People

Technology

1 A chance to reframe Internal Audit

2 Mandate

3 Strategic Plan

4 Board (Audit Committee) Engagement

5 Assurance Ecosystem

6 Performance Measures

7 Risk Assessment and Coverage

8 Audit Spectrum

9 Reporting and Communication

10 Capabilities