www.pwc.com/ca

IIA Lunch and Learn

April 11, 2024

pwc

www.pwc.com/ca

Agenda

1. Demystifying the Global Internal Audit Standards* update – 25 mins
2. Internal Audits Response to Gen AI – 25 mins
3. Questions – 10 mins

pwc

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

Focusing on the future: Introducing the new Standards

Session Overview

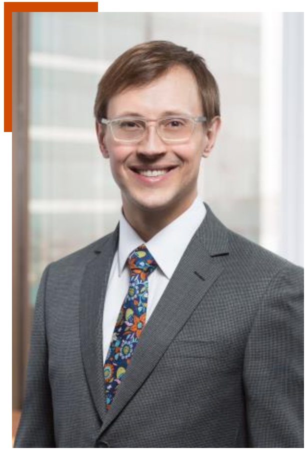
The Institute of Internal Auditors (IIA) revised its Global Internal Audit Standards™* ("the Standards") in 2023 to support the continued evolution of the profession and help organizations address today's complex risk landscape.

This represents a significant opportunity for Internal Audit (IA) functions to incorporate the latest developments in good practice and drive transformation to increase the value they can provide to their stakeholders.

All organizations will need to consider their response and implement changes for the new Standards in 2024, ready to conform in 2025.

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

Speakers



James Neale
Partner, Risk Assurance,
PwC Canada
james.j.neale@pwc.com

David Oberg
Senior Manager, Risk
Assurance, PwC Canada
david.oberg@pwc.com

An opportunity to transform: Key changes in the standards

The Standards, which can be found on the **IIA's global website**, include additional focus on areas such as:

- Board (or equivalent) involvement in IA
- IA mandate, vision and strategic plan
- An understanding of risks and coverage throughout the organization
- Planning, tracking and monitoring performance (e.g., efficiency and quality)
- IA reporting, ratings and effective communication

We note generally additional specificity and wording changes throughout the Standards along with a reorganization of the International Professional Practices Framework (IPPF).

A unified approach: How leadership should respond

The new Standards are not just relevant to IA - they impact the whole organisation. This means the Board and each line need to work together to capture the opportunities the new Standards bring. This includes:

Board/Audit Committee and Senior Management

Consider how a strong IA function can help the company achieve its vision by building resilience to protect value, and give the business confidence to transform to create value.

Questions to ask:

1. Has leadership had sufficient input to the IA plan on strategic priorities?
2. Can the new IIA Topical Requirements help us better focus on strategic risks?
3. Can we coordinate investment and effort across teams to get the best return on investment from the changes?

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

Capture the opportunity to align and collaborate with IA to strengthen the company's approach to risk and optimize assurance and monitoring activities.

Questions to ask:

1. Can we use assurance mapping to reassess risk coverage?
2. Where can joint training and upskilling enhance collective expertise on key risk areas?
3. What opportunities are there to collaborate with IA on approach, tools, technology and data?

IA Leaders (e.g., Chief Audit Executive)

Use the new Standards to continue the IA transformation journey and engage differently with stakeholders.

Questions to ask:

1. Is there an opportunity to refresh our IA strategy and align with the organization's latest objectives?
2. How can the new Standards help drive change in IA (people, processes and technology)?
3. How can benefits from implementing the new standards be measured and monitored?

Benefits - Unlocking the potential of IA

Organizations will be at different levels of maturity in relation to corporate governance and risk management. Critical to this is having a modern IA function that can adapt to a changing risk landscape and incorporate the latest Standards and best practices.

Based on the key areas of focus in the new Standards, benefits could include, for example:

- **Better stakeholder alignment -** through additional Board and Senior Management engagement in the IA life-cycle, alignment on strategic priorities and coverage, and optimized IA reporting.
- **More effective auditing of important risks** - incorporating IIA Topical Requirements and guidance to help IA enhance its approach to addressing key risk areas.
- **Increased efficiency and risk coverage** - by further cooperation with second line and a clear understanding of assurance activity mapped to key risk areas.
- **Additional insights and value to the business -** as a result of IA training and upskilling, including knowledge of strategic/business risks, audit methodology, and technology and data.

Highlights of New Requirements

New Key Areas of Focus

IA Mandate - required transparency with the Board (or equivalent e.g., Audit Committee) on the nature and types of services the IA function performs (i.e., do they cover the broad spectrum of organizational risks or are 90% SOX focused).

IA Strategic Plan - required transparency to management and the Board (or equivalent e.g., Audit Committee) of (1) the longer-term vision for the department, (2) annual objectives aimed at achieving that vision, and (3) formal reporting on progress against those goals. This includes both people/capability and technology goals and should be tied to budget requests.

Board Oversight - required Board approval for not just the IA charter and IA plan, but also the mandate, strategic plan, department budget and resource plan (requiring the CAE to at least annually discuss the headcount and capabilities of resources to deliver the plan and mandate with the Board), developed objectives and performance metrics, quality program (including approach to external assessments and direct receipt of full External Quality Assessment (EQA) report and approval of actions plans).

Coordinated Assurance - requirement to understand the organization's risks and internal and external providers of assurance services that cover those risks (e.g., assurance map).

Technological Resources - requires regular evaluation of technology used by IA function, to pursue opportunities to improve effectiveness and efficiency, and to report on any limitations caused by lack of technology to management and the Board (or equivalent e.g., Audit Committee).

Highlights of New Requirements

Board Oversight

Materials the CAE must communicate to the Board (or equivalent e.g., Audit Committee)

- IA charter (including IA mandate)
- Changes to the mandate or charter
- Potential impairments to independence
- Internal audit strategy
- IA budget
- Internal audit plan (including why high-risk areas are not included in the plan, if applicable)
- Annual confirmation of independence
- Internal audit and technological resources
- Quality assurance and improvement program plan & results
- External quality assessment plan, results (Board to receive directly from assessor) and action plans to address gaps
- Final engagement communications/results of internal audits
- Issue status and action plans

Highlights of some specific requirements that are new and more tactical in nature

Tactical Requirements.

- **Audit Plan**
  - Communicate to the Board/AC and senior management reasons high risk areas / activities are not included as an assurance engagement on the plan (as applicable)
- **Engagement Execution**
  - Engagement level risk assessment and documented work program
  - Evaluate significance of findings (consider likelihood and impact) and prioritize findings based on significance
  - Engagement conclusion must be developed to summarize significance of findings
  - Final communications include action owners and dates
  - Disclosures must be included if engagement was executed not in conformance with Standards
- **Quality Assessment(s)**
  - One member of the EQA assessor team must be a Certified Internal Auditor
  - Results of an EQA shared directly with the Board, include IA's action plans and report on progress
  - Annual communication of results of internal assessment

Topical Requirements and guidance to help IA functions focus on key risk areas.

- We understand that the full list of topics has not been finalized;
- Topical requirements on Cybersecurity to be issued for comment this month and released Q3;
- Other initially identified topics include Information Technology Governance, Privacy Risk Management, Sustainability and ESG, and Third-party Management.

A chance to reframe IA

5 key actions to drive change

There are five key steps involved in implementing the new Standards. We can help you maximize the value at every stage:

1. Assess readiness and agree priorities

Confidence in your response to the new Standards

- Perform an **IA Readiness Assessment** to identify what needs to change to conform with the new Standards.
- Discuss impact of changes with key stakeholders, including Board/Audit Committee, Senior Management, Risk and Compliance functions (e.g., in **stakeholder workshops**).
- Agree **actions and priorities** that will have the best outcomes for the organization.

2. Create transformation plan and refresh IA strategy

New opportunities to create value and forge stronger alignment

- Align actions and priorities to the organization's **vision, strategy, and governance model** and **update the IA Strategic Plan.**
- Create an **IA Transformation Plan** to achieve IA strategic plan and implement the new Standards, including key actions, success factors, resources, communication plan, and timeline.
- Incorporate **digital IA strategy** to embed technology changes to optimize IA and governance activities. This should include how IA will capture opportunities from **Artificial Intelligence (AI).**
- Map and agree **organizational dependencies** required to implement the plan, including Board/Senior Management input, investment, and cooperation of first and second line.

3. Implement the plan

Reaching the next stage of IA maturity

- **Implement plans;** which may include changes to:
  - IA's mandate and strategy
  - Coordination and collaboration with the second line
  - IA competencies and resource model
  - IA reporting and communications
  - Quality Assurance and Improvement Program (QAIP)
  - IA technology and data
- Reflect these changes in your **IA policies, procedures, and templates.**

4. Brief and train your people

Using the new Standards to unlock your IA 'superpowers'

- Refresh your **IA training and development program**, to reflect the new Standards.
- Incorporate the IIA's **new Topical Guidance.**
- Run stakeholder **briefings and workshops** to raise awareness, increase engagement, and embed behaviors (e.g., how to effectively manage more Board/Senior Management involvement and coordination with second line).

5. Monitor outcomes

Track and amplify successes for continual improvement

- Monitor achievement of **success factors and track IA Key Performance Indicators (KPIs)** to measure benefits.
- Obtain open **feedback from stakeholders** to gauge where they are getting the most value from the changes and amplify this across other areas, where appropriate.
- Fine tune QAIP activities in response to KPIs and feedback. Capture and implement additional improvements or factor into next IA plan.
- Prepare for the next **External/Strategic Quality Assessment** to independently check conformance with the new Standards.

Internal Audit's Response to Gen AI

Session Overview

Artificial Intelligence (AI) is rapidly changing how businesses operate worldwide. While it offers numerous benefits, it also brings up important questions about its impact and risks.

As AI technology keeps improving, organizations feel pressure to keep up, but alongside this fast progress, it's crucial to focus on building human skills like adaptability and learning. We need to understand how humans and AI can work together effectively.

There are risks involved in adopting AI, but there are also ways to manage them. By putting controls in place throughout the AI process, organizations can adopt AI with confidence. Having a plan to guide the journey toward AI can be helpful.

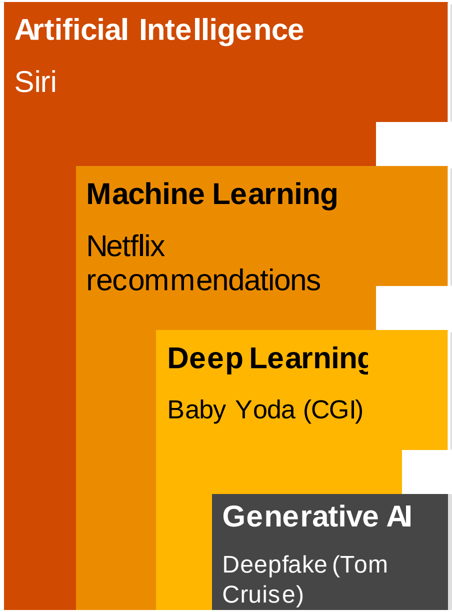
Speakers

James Neale
Partner, Risk Assurance,
PwC Canada
james.j.neale@pwc.com

Rahul Kohli
Partner, Technology Strategy
and Transformation,
PwC Canada
rahul.kohli@pwc.com

What is Generative AI?

Generative AI (GenAI) involves training a model to generate new data based on the training data it was given. This type of AI can be used to create music, text, and even virtual worlds, among other applications.



Artificial Intelligence

Siri

Machine Learning

Netflix recommendations

Deep Learning

Baby Yoda (CGI)

Generative AI

Deepfake (Tom Cruise)

Artificial Intelligence

the field of computer science that seeks to create intelligent machines that can replicate or exceed human intelligence.

Machine Learning

subset of AI that enables machines to learn from existing data and improve upon that data to make decisions or predictions.

Deep Learning

a machine learning technique in which layers of neural networks are used to process data and make decisions.

Generative AI

a capability of using prompts to create, improve, and interact with text, images, video, and sound using large trained models.

Why now?

In December 2022, ChatGPT, a chatbot application with GenAI capabilities, took the world by storm when OpenAI released access to the model online.

With **1M users in its first 5 days and 100M users in its first 60 days,** ChatGPT proved that there is a strong demand for these capabilities and has led innovators across every major industry to ask themselves how they can use the tool.

GenAI is ‘cognitively versatile’ and able to take on a broad range of ‘tasks’ across enterprises

Key Tasks that Generative AI can Tackle

	Summarize	Q&A	Improve	Improve	Q&A	Create
Tasks	**Summarization**	**Deep retrieval**	**Transformation**	**Augmentation**	**Q&A (Dialogue)**	**Net-new creation**
Examples	• Find key action items from meetings • Summarize articles and research papers • Summarize code documentation	• Find relevant content from firm's massive repository • Search regulatory documents to find important changes in regulation	• Translate text to a different language • Format code in line with standards • Personalize design per preference	• Impute missing values with synthetic data • Auto-complete code • Enhance client data with sentiment	• Respond to client queries with service options • Create reports from structured data based on QnA • Generate dialogue for in-product use	• Create images for marketing • Generate titles for articles • Generate code from textual description

However, there are significant Risks that need to be clearly understood

The use of artificial intelligence introduces risk across various facets of the organization. Understanding both the risks associated with the use of AI, as well as the use cases within the enterprise is a critical initial step during adoption. The major risk areas are listed below.

Cyber

When introducing AI to an organization, new threat vectors and potential security vulnerabilities must also be considered to ensure the organization is properly aligned to combat the new risks. Risks such as outdated security policies, insufficient training, and a new threat landscape.

Operational

Integration of AI can impact how organizations operate, including but not limited to business models, processes and the workforce. Risks include technical failures, challenges with integration, security risks, and lack of expertise.

Legal

As with any developments in technology, legal challenges are introduced with new laws and court decisions concerning AI. Examples of these risk are privacy violations, intellectual privacy disputes, and liability for damages.

Compliance

With AI comes rapidly evolving and complex regulatory frameworks, which can pose compliance risks for organizations seeking to adopt these technologies. Compliance risks to consider include data privacy regulations, regulations and internal policies.

Privacy

AI collects and process vast amounts of personal data, often without explicit consent or knowledge of individuals or organizations. Privacy risks include data breaches, surveillance, misuse of personal data and lack of transparency.

By prompting organizations and their internal teams who design, develop and deploy AI to think more critically about the potential risks and use cases, risk management can encourage responsible uses and practices.

Therefore, we believe it is critically important to take a responsible approach to the design and scaling of AI

Responsible AI (RAI) by Design

Embed responsibility at the heart of how you develop and use GenAI in your organization – using the four pillars of PwC's RAI framework as a foundation for designing your approach.

*** Our recent awards**

Worldwide Leader, **AI Services**, IDC MarketScape 2023
Leader, **AI Services**, Forrester Wave 2022
"Outstanding Achievement in the Field of **AI Ethics**", CogX 2020
"Outstanding Achievement in **Enterprise Adoption of AI**", CogX 2020

How responsible AI by design looks like in practice

Strategy

- Define what the ethical use of data means for your organization (e.g. what data can and can't be used) and embed it into your GenAI strategy
- Consider how your GenAI approach aligns with your organizational values and any regulatory & compliance requirements

Control

- Consider your governance, compliance and risk management practices as they relate to GenAI
- Assess what guardrails you have, need or must enhance to make sure you're using GenAI responsibly and mitigate risks

Responsible practices

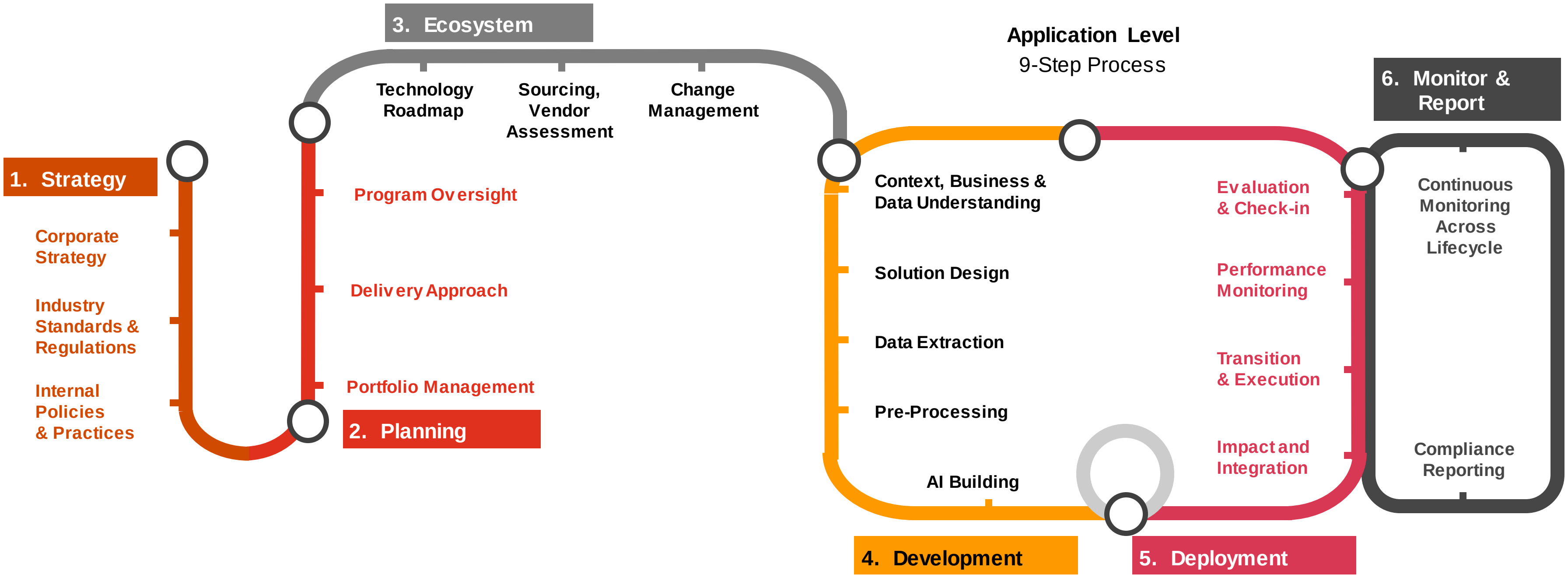
- Develop clear and transparent guidelines for how GenAI should be used in your organization
- Consider factors like explainability, robustness, bias and fairness, originality, security, privacy and safety

Core practices

- Develop overarching core practices to assess use cases and determine what type of AI to use (e.g. GenAI, AI/ML)
- Find ways to assess problems, identify industry best practices, and evaluate & improve AI performance while monitoring for innovations and regulatory changes

Responsible AI is not just a point in time

The foundation for responsible AI is an **end-to-end enterprise governance framework**, focusing on the risks and controls along your organization's AI journey—from top to bottom.



Existing governance models should be scalable and adaptable to match the pace of generative AI

GenAI council and charter	Set up council and charter or integrated with existing councils to support generative AI
Operating model	Develop operating model with associated RACI ownership across primary and supporting teams
Policies and standards	Incorporate GenAI considerations into existing cybersecurity, regulatory, and AI and data policies and standards
Risk and controls matrix	Include guidance from industry frameworks and global and domestic regulations
Model testing and validation	Continuously review and refine models for reliability, bias/fairness, privacy, transparency etc.

Additional Considerations

1. Establish a governance structure and enterprise-wide generative AI risk management framework
2. Engage with the leading AI technology providers
3. Perform legal diligence on your contracts and intellectual property
4. Engage your employees in identifying use cases in their work and for the company's customers
5. Evaluate and prioritize use cases based on risk/reward. Look for common "patterns" that apply to the majority of use cases, are reusable and applicable to future use cases. Start with those use cases.
6. Build your central generative AI with tooling and enhancements as well as the appropriate security and controls
7. Do trial runs in sprints
8. Roll out for broader use under a dedicated enterprise program office
9. Monitor your foundation models and applications for compliance and drift periodically, using a model governance tool such as Model Edge, a PwC Product
10. Adopt effective generative AI systems and model metrics; and monitor for "concept drift," toxicity and bias

Generative AI in Internal Audit

	Risk Assessment	Planning	DEA	OET	Reporting	Issue Management
Internal audit lifecycle	• Perform annual risk assessment • Create audit plan • Determine AU/AC	• Start with scope developed from risk assessment • Conduct walkthroughs • Document process narratives and process flows • Develop risk and control matrix (RCM)	• Perform control design assessments • Update RCM and draft testing steps • Confirm identified issues	• Perform testing of controls effectiveness or data analysis to identify anomalies • Confirm identified issues	• Draft observations and recommendations • Collect management action plans and targeted implementation dates • Draft final audit report	• Obtain management responses to action plans and sign-offs • Evaluate whether issue has been appropriately remediated
How Gen AI can innovate	Risk Assessment Co-pilot	Planning Memo Automation	Process Narrative Automation	Testing Workpaper Generation	Audit Report Co-pilot	Continuous Monitoring
	Regulatory Change Summarization	Risk and Control Matrix Generation	Testing Steps Generation	Testing Automation	Thematic Issue Summarization	Emerging Risk Identification

Where internal audit is now…	… how generative AI can transform
Significant manual effort is expended reading documents to confirm required elements are present	Perform document Q&A with a natural language interface, as if you're working with a chatbot that **instantly reads and understands** your documents
Automation only applies for highly rote, non-reasoning, transactional data testing	**Machine learning** reads and applies test procedures in a **single step**
Workpaper development is a low-value, high-cost activity	Summarizing test procedures and **generating workpapers** is performed by **artificial intelligence**

Challenges of AI adoption in internal audit

Who owns the risk?

Challenge: Internal audit solutions should not change the ownership and accountability of risk mitigation.

Solution: Establish tech collaboration outside of internal audit, develop solutions that can be leveraged by other Lines. The overall governance of AI should include cross function support and oversight far beyond internal audit and technology teams.

Who validates the AI solution?

Challenge: Internal audit-owned models may present a conflict of interest if validated by model risk management (MRM).

Solution: Establish independent validation groups to support internal audit and confirm appropriate data and technology controls exist.

How is return on investment (ROI) measured?

Challenge: Metrics to measure ROI on AI solutions is often limited to cost/time savings.

Solution: Define a benefits framework to capture metrics that demonstrate ROI across different categories (e.g., risk coverage, audit findings, external criticisms)

How will internal audit validate solutions developed by the business

Challenge: Internal audit has to be able to validate other Lines (e.g., 2nd Line) solutions if these solutions have a direct impact on the audit.

Solution: Establish methodology and retain the right expertise to perform AI model validations.

How do you develop and deploy AI solutions with limited time and budget?

Challenge: Tight timelines and capacity constraints create barriers to technology adoption.

Solution: Identify and prioritize solutions that impact a range of audits to provide greater ROI against the investment.

What skill is needed for internal audit?

Challenge: Internal audit may lack the necessary skills to adopt AI.

Solution: Internal audit should perform a skill assessment to understand gaps and plan for upskilling and/or obtaining outside support.

Source: PwC, Harnessing the power of AI in IA

Q&A

Thank you

pwc.com/ca

PwC refers to the Canadian firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisers.