Integrated GRC & AI Governance for Internal Auditors

Johannesburg: 26 to 27 August 2026

Cape Town 9 to 10 September 2026

Both events will be blended with online participation

Prices all inclusive

Per Person	R6 500
Groups of 2+	R5 500
Online	R4 500

Book now!

"The future of governance is not choosing between AI and control. It is ensuring AI accelerates performance without compromising ethics, compliance or resilience. Internal Audit is uniquely positioned to provide that independent assurance that helps the organization achieve its mission-critical objectives responsibly.

COURSE OVERVIEW

Artificial intelligence is rapidly changing the environment in which internal audit operates. AI is increasingly embedded in strategic decision-making, financial and operational processes, customer interactions, fraud detection, cybersecurity, human resources, data analytics and automated decision-making. For internal audit, the challenge is no longer simply to understand AI. The profession must be able to provide credible and independent assurance over **how AI is governed, how its risks are managed and whether the controls surrounding AI-enabled processes are appropriately designed and operating effectively**.

PRESENTERS

Dr Dirk Brand | Deon van der Westhuizen

COURSE OUTCOMES

By the end of this masterclass, participants will be able to:

- **Identify** where AI is being used across the organisation and determine which AI applications warrant internal audit attention.
- **Assess** AI governance and accountability using King V as the overarching governance baseline.
- **Apply** ISO/IEC 42001 as a structured basis for evaluating the organisation's AI management system and assurance readiness.
- **Use** COSO, NIST AI RMF and COBIT as complementary criteria when assessing AI-related governance, risk and controls.
- **Evaluate** material AI risks including bias, privacy, cybersecurity, hallucination, model drift, explainability, data quality, regulatory exposure and third-party dependency.
- **Assess** data governance, model governance, human oversight, monitoring, audit trails and third-party AI arrangements.
- **Clarify** the respective responsibilities of the first, second and third lines for AI governance, risk management and assurance.
- **Develop** an integrated AI assurance map that identifies assurance gaps, duplication and opportunities for reliance.
- **Design** a risk-based internal audit engagement for an AI-enabled process.
- **Evaluate** the design and operating effectiveness of AI-related controls.
- **Report** significant AI governance, risk and control matters in the context of mission-critical organisational objectives.
- **Develop** an AI assurance dashboard suitable for reporting to the Audit Committee.
- **Build** a 90-day roadmap for strengthening the internal audit function's AI assurance capability.

WHO SHOULD ATTEND

Chief Audit Executives, Internal Audit Managers, Senior Internal Auditors, IT Auditors, Technology Auditors, Cybersecurity Auditors, Data and Analytics Auditors, Combined Assurance Specialists, Risk and Assurance Professionals, and Audit Committee Members.

DAY 1: AUDITING THE AI GOVERNANCE ENVIRONMENT

Session 1: The Changing Internal Audit Mandate in an AI-Enabled Organisation

Understanding how AI changes the organisational risk universe | Identifying AI-enabled activities across business processes | Recognising generative AI, predictive analytics and automated decision-making as emerging assurance areas| Identifying approved, embedded and potentially unapproved or shadow AI | Connecting AI use to strategy, performance and mission-critical objectives | Assessing the potential impact of AI on value creation and value preservation | Understanding how AI changes existing financial, operational, compliance, technology and reputational risks | Determining when AI becomes sufficiently material to require internal audit attention | Considering the implications of AI for the internal audit universe and risk-based audit plan | Maintaining internal audit independence and objectivity when internal audit itself uses AI

Practical Exercise: Participants map where AI could exist across a typical organisation and develop an initial **AI Audit Universe**, linking AI applications to business processes, mission-critical objectives, material risks and potential assurance requirements.

Session 2: Auditing AI Governance Using King V

Applying King V as the governance baseline for assessing AI oversight | Evaluating ethical and effective leadership in AI-related decision-making | Assessing governing body oversight of technology and information | Determining whether accountability for AI has been clearly established | Evaluating the relationship between AI governance and organisational purpose | Assessing whether AI supports sustainable value creation and preservation | Evaluating stakeholder considerations in AI-enabled decisions | Assessing transparency and disclosure relating to AI systems and their outcomes | Evaluating governance structures for responsible AI deployment | Determining whether significant AI risks are appropriately escalated to executive management and the governing body | Assessing whether the governing body receives sufficient and reliable information to discharge its oversight responsibilities

Practical Exercise: Participants conduct a **King V AI Governance Gap Assessment**, examining a hypothetical organisation's AI governance arrangements and identifying potential governance weaknesses, audit evidence requirements and matters that may need to be reported to the audit committee.

Session 3: Navigating the AI Governance Framework Ecosystem from an Internal Audit Perspective

Positioning King V as the overarching governance anchor | Understanding ISO/IEC 42001 as the structural foundation for an AI management system | Applying COSO to enterprise risk management and internal control | Using NIST AI RMF to understand the Govern, Map, Measure and Manage dimensions of AI risk | Positioning COBIT within technology and information governance | Applying the Three Lines Model to accountability and independent assurance | Understanding how the frameworks complement rather than compete with one another | Selecting appropriate criteria for different types of

AI audit engagements | Connecting governance principles to operational controls and audit evidence | Integrating AI assurance into the broader GRC and combined assurance architecture

Practical Exercise: Participants develop an **AI Governance Framework Alignment Map** showing how the different frameworks contribute to: **Governance → Risk Management → Technology Governance → AI Management → Internal Control → Assurance.** The exercise requires participants to identify which framework provides the most appropriate audit criteria for different aspects of an AI-enabled environment.

Session 4: Auditing ISO/IEC 42001 and the AI Management System

Understanding the purpose and structure of an AI management system | Assessing the scope of the organisation's AI management arrangements | Evaluating AI policies and governance requirements| Assessing defined roles, responsibilities and ownership | Evaluating AI risk assessment processes | Reviewing AI impact assessment practices | Assessing controls across the AI lifecycle | Evaluating governance over design, development and acquisition | Assessing deployment, operation and ongoing monitoring | Reviewing change management and model updates | Assessing decommissioning and retirement of AI systems | Evaluating documentation, evidence retention and audit trails | Assessing monitoring, corrective action and continual improvement | Determining readiness for internal and external assurance

Workshop: Participants review a hypothetical AI management system against the core governance and management requirements of ISO/IEC 42001. They identify control gaps; determine the audit evidence required and formulate potential internal audit observations.

Session 5: The Three Lines Model, Integrated Assurance and Internal Audit Independence

Clarifying management's ownership of AI risks and controls | Defining first-line responsibilities for AI-enabled processes | Understanding second-line oversight by risk management, compliance, legal, cybersecurity, privacy and data governance | Defining internal audit's independent third-line assurance role | Protecting internal audit independence when advising on emerging AI governance arrangements | Distinguishing advisory work from assurance engagements | Mapping assurance activities across the Three Lines Model | Assessing the quality and reliability of assurance provided by other functions | Determining when internal audit can place reliance on other assurance providers | Identifying assurance gaps and unnecessary duplication | Considering specialist and external assurance for technically complex AI risks | Establishing escalation and reporting mechanisms for material AI governance weaknesses | Connecting AI assurance to the organisation's broader combined assurance approach

Practical Exercise: Participants develop an **AI Combined Assurance Map** structured around: **Mission-Critical Objective → AI Risk → Key Control → Control Owner → First-Line Monitoring → Second-Line Oversight → Third-Line Assurance → External Assurance → Assurance Gap.** Participants identify areas of over-assurance, under-assurance and duplication and determine where internal audit should provide independent assurance.

DAY 2: AUDITING AI RISK, CONTROLS AND ASSURANCE

Session 6: Building the AI Risk Universe

Bias and discrimination in AI-supported decisions | Privacy and protection of personal information | Cybersecurity threats affecting AI systems and data | Hallucination, accuracy and reliability of AI-generated outputs | Model drift and deterioration in model performance | Lack of explainability and transparency | Poor data quality, integrity and lineage | Regulatory and compliance exposure | Third-party AI and vendor dependency | Reputational risk and AI washing | Workforce disruption and inappropriate automation | Over-reliance on AI without adequate human oversight | Ethical risks and unintended stakeholder consequences

Workshop: Participants assess a hypothetical AI implementation, identify root causes and consequences, determine inherent risk, evaluate existing controls and assurance activities, and assess residual risk.

Session 7: Auditing AI Controls – General Controls and Application Controls

AI governance and oversight controls | User access and authorisation controls | Data governance and data quality controls | Model development, approval and validation controls | Change management and version control | Preventive, detective and corrective controls | Automated versus manual controls | Human-in-the-loop and human-on-the-loop controls | Exception management and escalation | Model performance and drift monitoring | Logging, audit trails and traceability | Incident management and corrective action.

Participants develop an **AI Risk and Control Matrix** for an AI-enabled business process, linking:
Objective → Inherent Risk → Root Cause → Control Process → Preventive Controls → Detective Controls → Level of Automation → Residual Risk → Assurance Response

Session 8: Auditing Data, Models and Third-Party AI

Data ownership and accountability | Data quality, completeness, accuracy and integrity | Data lineage and traceability | Training, validation and operational data | Model approval and independent validation | Model performance and monitoring | Model drift and performance thresholds | Changes to models and algorithms | Third-party AI providers and vendor dependency | Contractual controls and accountability | Cloud-based and externally hosted AI solutions | Availability and reliability of audit evidence | The appropriate use of technical specialists and other assurance providers

Participants conduct an internal audit review of an organisation using a third-party AI solution. They identify key risks, control weaknesses, evidence requirements and areas where internal audit may need to rely on specialist or external assurance.

Session 9: Designing and Executing the Risk-Based AI Internal Audit

Defining the audit objective and scope | Linking the audit to mission-critical organisational objectives | Identifying the AI systems and processes within scope | Establishing suitable audit criteria | Using King V, ISO/IEC 42001, COSO, NIST AI RMF and COBIT as sources of audit criteria | Developing the AI audit programme | Identifying key controls for testing | Testing control design and operating effectiveness | Using data analytics and continuous auditing | Evaluating governance and accountability | Determining when specialist technical expertise is required | Developing findings based on root cause, risk, control weakness and organisational impact

Participants design a **risk-based internal audit programme for an AI-enabled process**, including audit objectives, key risks, expected controls, audit procedures, evidence requirements and reporting criteria.

Session 10: Reporting AI Assurance to the Audit Committee and the Internal Audit AI Roadmap

Reporting AI risk in the context of mission-critical objectives | Translating technical findings into governance and business implications | Distinguishing isolated control weaknesses from systemic governance failures | Reporting significant residual AI risk | Communicating limitations in assurance coverage | Developing meaningful AI key risk and assurance indicators | Reporting emerging and interconnected AI risks | Identifying gaps and duplication across assurance providers | Integrating AI into the annual and rolling internal audit plan | Building AI capability within the internal audit function | Determining when to develop, recruit or source specialist capability | Moving towards continuous assurance over high-risk AI environments

Final Practical Exercise: Participants develop an **Audit Committee AI Assurance Dashboard** covering: **Mission-Critical Objective → Material AI Risk → Key Controls → Control Effectiveness → Assurance Provider → Assurance Coverage → Residual Risk → Internal Audit Conclusion → Required Action**

The masterclass concludes with each participant developing a **90-Day Internal Audit AI Assurance Roadmap**, identifying the immediate actions required to assess their organisation's AI exposure, update the audit universe, identify assurance gaps, strengthen internal audit capability and incorporate material AI risks into future audit planning.