
Risk-Based Internal Auditing: Advanced Practice

11 – 15 January 2027
Rome





Risk-Based Internal Auditing: Advanced Practice

Ref: 1805_6017 **Date:** 11 – 15 January 2027 **Location:** Rome **Fees:** 5500 GBP

Programme Summary

Traditional compliance checklists and fixed calendar cycles often misallocate examination resources across non-critical operations. Risk-Based Internal Auditing aligns supervisory reviews with strategic vulnerabilities, establishing disciplined linkages between corporate threat registers, enterprise appetite thresholds, and targeted fieldwork. Practitioners evaluate controls against material business exposure, transitioning evaluation routines from reactive inspection to predictive appraisal. This intensive masterclass is delivered by Mars Training Centre UK.

The Business Case

Organisations facing fast-moving operational and regulatory environments cannot afford static review cycles that waste capacity on low-impact entities. By calibrating supervisory activities directly to measurable exposures, enterprises enhance control efficacy and safeguard institutional capital.

- **Resource Prioritisation:** Directs substantive testing hours toward entities displaying heightened residual exposure.
- **Framework Alignment:** Embeds corporate appetite thresholds and enterprise indicators directly into scope memoranda.
- **Defensible Assurance:** Generates objective, repeatable testing rationale that satisfies governance bodies and external examiners.
- **Early Threat Detection:** Identifies emerging operational vulnerabilities before systemic control breakdowns occur.

Principles and Evidence Base

- **Global Internal Audit Standards:** Establishes mandatory performance requirements for planning and executing risk-calibrated engagements.
- **COSO Enterprise Risk Management:** Integrates core enterprise risk management principles with internal control evaluation.
- **ISO 31000:2018:** Informs risk criteria, assessment protocols, and structured risk treatment verification across all review stages.



Intended Participants

- Mid-level and senior review practitioners seeking to ground fieldwork in modern risk prioritisation frameworks.
- Methodology specialists and engagement leads responsible for scoping annual examination schedules.
- Control professionals and risk analysts transitioning into substantive internal review responsibilities.
- Assurance officers tasked with modernising traditional inspection programmes into risk-calibrated workflows.

The curriculum directly supports professionals operating across regulated sectors, corporate infrastructure, supply networks, and commercial institutions.

Learning Outcomes

1. Participants will be able to align supervisory scopes with enterprise appetite statements and threat registers.
2. Participants will be able to apply the COSO ERM framework and ISO 31000 principles to universe prioritisation.
3. Participants will be able to construct dynamic entity scores reflecting residual vulnerability and operational volatility.
4. Participants will be able to design risk-ranked substantive testing matrices and automated sampling routines.
5. Participants will be able to execute root-cause diagnostics on systemic control deficiencies.
6. Participants will be able to communicate prioritised findings and residual exposures to executive oversight committees.

Programme Structure

Day 1: Methodological Architecture and Enterprise Alignment

How are risk management standards translated into an operational examination methodology?

- Principles of Risk-Based Internal Auditing versus traditional cyclical testing
- Global Internal Audit Standards governance and risk-calibration mandates
- COSO ERM framework integration and risk-appetite mapping
- ISO 31000:2018 principles applied to engagement design
- Establishing risk criteria, materiality thresholds, and appetite boundaries

Day 2: Universe Calibration and Dynamic Engagement Scoping

How is an auditable universe structured, weighted, and maintained over time?



- Constructing the auditable entity register and defining boundary criteria
- Inherent risk rating, velocity analysis, and vulnerability scoring
- Control environment maturity evaluation and residual exposure calculation
- Dynamic annual scheduling versus rolling risk-adjusted prioritisation
- Drafting risk-focused engagement planning memoranda

Day 3: Control Design Evaluation and Threat Walkthroughs

How are individual process threats identified, linked, and tested for design adequacy?

- Process decomposition and risk-and-control matrix RCM construction
- Key risk indicators KRIs as triggers for targeted field evaluations
- Executing process walkthroughs to test preventative and detective control design
- Evaluating automated and manual controls across operational workflows
- Identifying control gaps, redundant activities, and unmitigated exposures

Day 4: Risk-Ranked Substantive Testing and Automated Sampling

How do practitioners structure fieldwork to validate operating effectiveness?

- Risk-proportional sample size determination and sampling methodologies
- Data-driven field testing using analytics and anomaly detection
- Testing high-impact controls through substantive evidence gathering
- Evaluating third-party dependencies, system permissions, and operational handoffs
- Documenting defensible working papers aligned with professional criteria

Day 5: Issue Prioritisation, Root Cause Analysis, and Continuous Assurance

How are findings analysed, weighted, and translated into management action?

- Structured root cause analysis protocols using Ishikawa and five-why techniques
- Impact-calibrated issue severity rating and residual risk reporting
- Designing corrective action plans with verifiable risk reduction metrics
- Continuous monitoring mechanisms and early warning alert triggers
- Constructing executive-level assurance summaries and trend analyses

Methodology

The sessions employ a workshop-driven approach combining technical analysis, process mapping, and real-world case simulations. Participants work through realistic scenarios to calibrate scoring templates, construct risk-and-control matrices, and design defensible testing schedules.

- Suggested activity: Calibrating a multi-factor risk scoring model to rank a sample portfolio of operational divisions.
-



Suggested activity: Formulating a complete risk-and-control matrix for a complex cross-functional workflow.

- Suggested activity: Conducting a structured root cause analysis on a recurring operational control failure.

Capstone Output

Each participant constructs a comprehensive risk-based engagement pack, including an operational risk-and-control matrix, an evidence-backed sampling plan, and a risk-prioritised reporting template. This output provides an operational baseline that attendees can immediately implement to modernise their organisation's internal review workflows.

Frequently Asked Questions

How does this methodology differ from standard compliance reviews?

Standard compliance reviews assess conformity to fixed rules regardless of context, whereas this approach allocates testing effort dynamically based on the likelihood and magnitude of operational impact.

Are specific technical tools or software packages required?

No specific proprietary software is required. The analytical techniques and scoring matrices are designed to be applied using standard spreadsheet tools or integrated governance software platforms.

How does this course address rapidly shifting corporate risk profiles?

The curriculum emphasises continuous monitoring, risk velocity tracking, and rolling schedule updates, enabling teams to adjust field priorities as emerging risks arise.

Can the templates provided be customised for specific industries?

Yes. All risk matrices, scoring criteria frameworks, and sampling schedules are provided in adaptable formats suitable for implementation across varied operating models.