BREAKING THE SILOS: ENTERPRISE RISK MANAGEMENT IN AUDITING

'From Hindsight to Foresight: Transforming Audit through Integrated Risk Intelligence'

Agenda

01 Common Risk Misconceptions

02 Risk Articulation Challenges

03 Risk Assessment & Evaluation

04 Joint Risk Assessments & Controls

05 Coordinating Assurance Providers

06 Risk-based Decision Making

We couldn't load the Menti slide

Exit slideshow mode, then select the Menti slide you want to add. After selecting it, start the slideshow again.

If the issue persist, please reach out to us at help@mentimeter.com

UNDERSTANDING RISK: DEFINITIONS & MISCONCEPTIONS

IRM	ISO 31000:2018	Hillson, 2016
The combination of the probability of an event and its consequence — ranging from positive to negative.	*The effect of uncertainty on objectives. An effect is a deviation from the expected — positive, negative, or both.*	*Uncertainty that matters.*
Risk = Uncertainty	Opportunity is positive risk	Eliminating all risk eliminates growth

💡 Key Insight: Risk is not just a threat — it also encompasses uncertainty that can lead to positive outcomes. Effective auditors recognize both dimensions.

Sources : ISO 31000:2018 . IRM Risk Definition, David Hillson, COSO ERM 2017

RISK AS OPPORTUNITY: CORPORATE LESSONS

KODAK — INVENTED THE FUTURE, THEN BURIED IT

In 1975, Kodak engineer Steve Sasson invented the digital camera — but executives shelved it to protect their $10B film business. They saw digital as a threat to profits, not the opportunity it was. By 2012, Kodak filed for bankruptcy while the technology they created became universal.

BLOCKBUSTER — TURNED DOWN NETFLIX FOR $50M

In 2000, Netflix founders offered to sell for $50 million. Blockbuster's CEO laughed them out of the room, viewing streaming as a risky niche — not a market shift. By 2010, Blockbuster was bankrupt. Netflix is now worth over $250 billion.

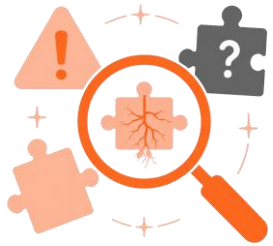
NOKIA — FEARED CANNIBALIZING ITS OWN SUCCESS

Nokia dominated 40% of the global phone market but refused to pivot to smartphones, fearing it would undermine their profitable feature phone business. Apple and Android seized the opportunity Nokia rejected. By 2014, Nokia's handset division was sold to Microsoft.

Risk Articulation

Precise language is the foundation of effective risk management

Causes – WHY?



Source
Immediate cause or origin

Underlying Threat
As a result of / Due to / Because...

Risk – WHAT?

Risk Event

Consequences – WHAT WILL HAPPEN?

Impact
Direct business consequence

Effect
May lead to...

Reproduced based on 'The Orange Book' – Management of Risk Principles and Concepts

Risk Articulation

Key enabler – shared risk taxonomy

Root Cause

WHY IT HAPPENS?

The underlying source or trigger that creates the risk

Examples:

1. Weak password policy
2. No dual-approval
3. Untrained staff
4. Legacy systems
5. Manual process

Where to place PREVENTIVE controls

Risk Event

WHAT HAPPENS?

The specific, identifiable occurrence that may happen

Examples:

1. Unauthorized wire transfer
2. Ransomware attack
3. Data breach
4. Mis-booked trade
5. AML violation

What to describe precisely in the risk register

Consequence

WHAT COULD HAPPEN?

The impact or outcome if the risk event materializes

Examples:

1. $2M fine
2. Financial loss
3. 48hr outage
4. Regulatory sanction
5. Lost customers

Where to assess IMPACT severity 'So What?'

Casual Chain

How Risk is Derived: The Causal Chain

Root Cause ⚠ WHY?

Conditions or failures causing risk events. Can be internal like human error or external like market shifts. Identifying these helps prevent risks.

- Root cause analysis
- Identify vulnerabilities
- Preventative plans
- Example: Poor staff training on data handling

Risk Event 🔗 WHAT?

The uncertain event that may occur if root causes persist. This is where threats like data breaches or system failures happen.

- Risk event descriptions
- Likelihood & impact
- Event scenarios
- Example: Unauthorized data access due to poor training

Consequence 🎯 IMPACTS

Outcomes from risk events affecting objectives, such as financial loss or reputational harm. Helps prioritize mitigation.

- Impact analysis
- Continuity plans
- Mitigation strategies
- Example: Financial loss from data breach

Risk Articulation – Practical Examples

Risk Statement Formula: Risk of [Event] due to [Root Cause], leading to [Consequence]

	Segregation of Duties	Fraud	Money Laundering	Cyberattack
Cause: Due to	Lack of SoD in payment approvals	Inadequate vendor due diligence	Poor KYC &DD	Weak endpoint security
Risk Event: There is a risk that	Unauthorized transactions	Procurement Fraud	FI will be used to launder money	Ransomware attacks on customer databases
Impact: May result in	Financial & reputational losses	Financial & reputational losses	Substantial Fines and even loss of license	critical data loss

	Cyberattack	Cyberattack	Human Error	Human Error
Cause: Due to	Unpatched software vulnerabilities	Insufficient email filtering	Manual data entry errors during loan origination	Failure to follow reconciliation procedures
Risk Event: There is a risk that	Unauthorized system access	Phishing campaigns to succeed	Inaccurate records	Undetected discrepancies
Impact: May result in	Theft of sensitive client data.	Credential compromise and fraud.	Financial misreporting	Material misstatments

RISK MANAGEMENT CYCLE

A structured four-step approach to managing risk

Risk Capacity, Tolerance & Appetite

Cost-Benefit Analysis

Informed Risk Decisions

01 Define Context & Objectives

Define and Understand the external and internal context in which the Organization/Structural Unit/ Entity/ Audit Subject is operating

02 Define Context & Objectives

Identify inherent risks as well as potential/emerging risks related to the objectives (both threats and opportunities). Analyze risks to find out the scale of the risks, evaluate risks to determine further actions whether they are acceptable or whether actions are needed to manage them

03 Monitor, Review, Report

Monitoring and reviewing the status of risks, risk responces, causes, consequences, corrective actions if any, changes in the context and objectives. Reviewing the effectivness of controls and provide effective risk reporting to all keystakholders.

04 Monitor, Review, Report

Identify relevant responses to the risks: 4 T.

We couldn't load the Menti slide

Exit slideshow mode, then select the Menti slide you want to add. After selecting it, start the slideshow again.

If the issue persist, please reach out to us at help@mentimeter.com

RISK TREATMENT– The 4 Ts Framework

Selecting the right response based on likelihood and impact

Transfer — Outsource / Insure

Shift the risk to a third party via insurance, outsourcing, or contractual arrangements.

📍 High Impact / Low Likelihood

Terminate — Avoid / Eliminate

Stop the activity generating the risk entirely. Used when risk is unacceptable and cannot be mitigated.

📍 High Impact / High Likelihood

Tolerate — Accept / Retain

Accept the risk when the cost of treatment exceeds the expected benefit. Monitor and review regularly.

📍 Low Impact / Low Likelihood

Treat — Control / Reduce

Implement controls to reduce either the likelihood or impact of the risk to an acceptable level.

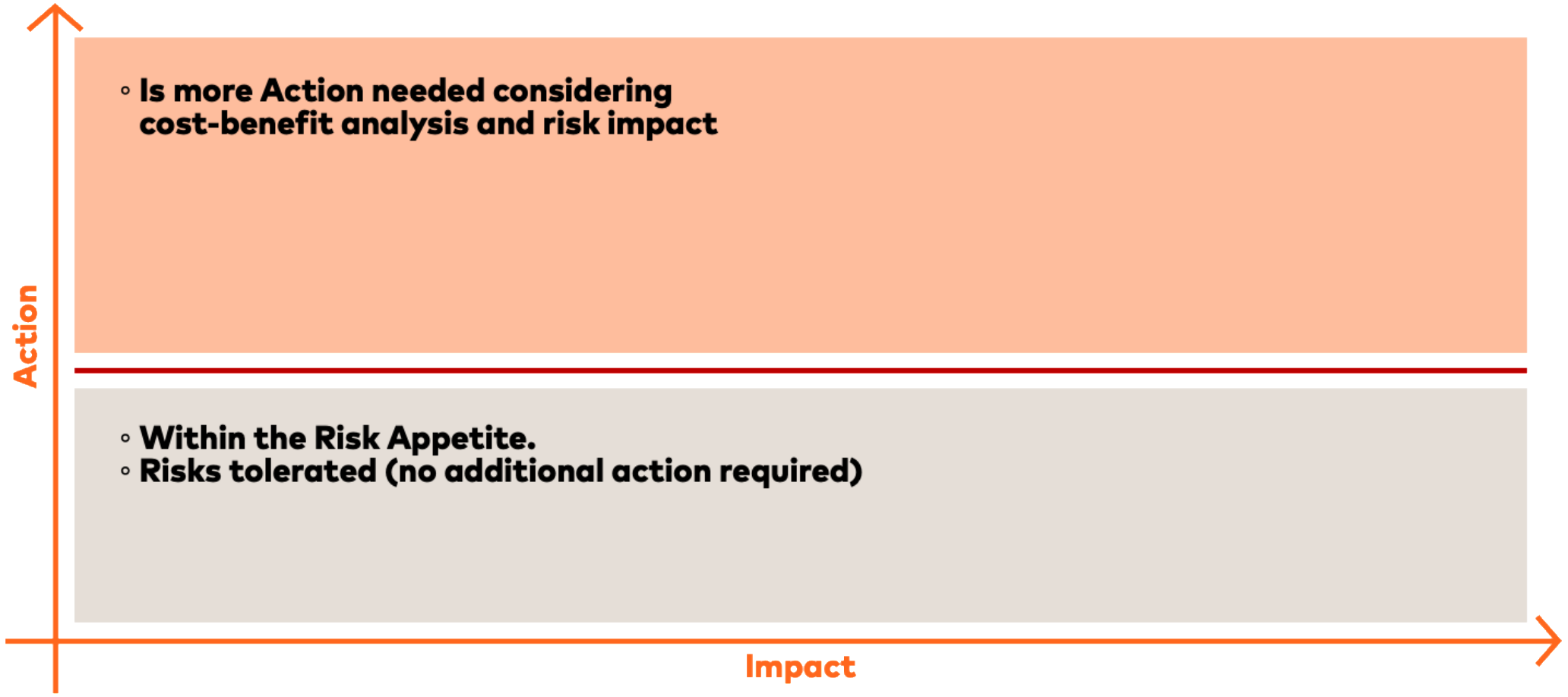
📍 Low Impact / High Likelihood

Likelihood

Impact

COST – BENEFIT ANALYSIS

Selecting the right response based on impact and feasibility



RISK- BASED DECISION MAKING

Risk Intelligence

RISK PRIORITIZATION FRAMEWORKS

Likelihood-impact matrices, heat maps, and risk scoring models help leadership objectively rank risks, ensuring resources target the most critical exposures and audit plans are evidence-based.

DATA-DRIVEN RISK INTELLIGENCE

Continuous monitoring, advanced data analytics, and real-time Key Risk Indicator (KRI) dashboards provide early warnings of emerging risks, shifting audit focus from past events to future threats.

DECISION SUPPORT TOOLS

Interactive risk dashboards and scenario analysis tools empower decision-makers with clear insights, enabling rapid adjustments to risk responses and audit priorities as conditions evolve.

CULTURE OF RISK AWARENESS

Embedding risk intelligence into organizational culture promotes proactive risk identification and responsiveness, ensuring all levels of the organization contribute to dynamic risk management.

JOINT RISK ASSURANCE

WHY IT MATTERS

Integrating assurance across all three lines eliminates blind spots, reduces duplication, and delivers a unified view of risk to the board and executive leadership.

THE RATIONALE

Siloed assurance functions may fail to address critical organizational risks. Joint risk assurance creates a unified framework that aligns management controls, compliance, and internal audit. This provides the Audit Committee with complete assurance of the organization's risk coverage

COORDINATING ACROSS THE THREE LINES

Joint Planning
Align audit calendars, share risk assessments, define coverage boundaries

Shared Platforms
Common GRC tools, unified risk taxonomy, integrated reporting dashboards

Reliance Protocols
Formal agreements on leveraging each line's work to avoid duplication

Continuous Dialogue
Quarterly coordination forums, escalation pathways, real-time alerts

Governance & Escalation: A robust governance structure requires regular coordination among all assurance providers. We recommend that these functions meet no less than quarterly to identify coverage gaps, deconflict overlapping activities, and approve collaborative assurance plans.

KEY BENEFITS

Eliminates Coverage Gaps
Systematic mapping ensures every risk domain has appropriate assurance from at least one line

Optimizes Resources
Leveraging reliance models reduces redundant testing and frees capacity for emerging risks

Reduces Audit Fatigue
Coordinated schedules and shared workpapers minimize disruption to business operations

Accelerates Response
Shared intelligence and escalation protocols enable faster reaction to emerging threats

Strengthens Board Reporting
Unified assurance view enables the Audit Committee to assess residual risk with greater precision

Improves Risk Culture
Cross-functional collaboration embeds risk awareness deeper into operational decision-making

KEY CHALLENGES

Independence vs. Collaboration
Internal audit must maintain objectivity while actively coordinating — formal protocols and clear reporting lines are essential to preserve independence standards.

Cultural & Organizational Resistance
Functions accustomed to working autonomously may resist transparency; executive sponsorship and incentive alignment are critical to overcome inertia.

Data & Technology Fragmentation
Disparate GRC systems, inconsistent risk taxonomies, and siloed data prevent real-time visibility — a unified platform strategy is a prerequisite.

Resource & Timing Conflicts
Competing priorities across lines can derail joint planning; a dedicated coordination function with authority to resolve scheduling conflicts is necessary.

COLLABORATIVE ASSURANCE

Joint Risk Assessment & Shared Control Testing

UNIFIED RISK UNIVERSE

Establishing a consolidated risk universe that integrates perspectives from internal audit, risk management, and compliance ensures comprehensive coverage and a shared understanding of organizational threats.

COLLABORATIVE ASSESSMENT FRAMEWORK

A structured framework for joint risk assessment aligns methodologies, scoring criteria, and prioritization across assurance functions, enabling consistent evaluation of risk severity and likelihood.

SHARED CONTROL TESTING

Coordinating control testing activities across assurance providers reduces redundant procedures and audit fatigue while maintaining rigorous coverage of key controls and compliance requirements.

ELIMINATING DUPLICATION

Mapping overlapping audit activities and consolidating testing efforts eliminates unnecessary duplication, freeing resources for higher-value assurance work and strategic risk advisory.

COORDINATING WITH OTHER ASSURANCE PROVIDERS

Integrated Assurance

EXTERNAL AUDITOR ALIGNMENT

Establish regular liaison meetings with external auditors to share risk assessments, align audit scopes, and agree on areas where internal audit work can be relied upon, reducing external audit hours and fees.

REGULATORY COORDINATION

Proactively engage regulators by sharing the internal audit plan and key findings. Demonstrating a robust ERM framework builds regulatory confidence and influences examination timing and focus.

COMPLIANCE TEAM INTEGRATION

Synchronize audit and compliance calendars to prevent overlapping activities, share findings promptly, and jointly address compliance risks for a unified control environment.

RISK MANAGEMENT PARTNERSHIP

Collaborate with risk management teams to integrate risk insights and mitigation strategies into audit planning, ensuring comprehensive coverage of emerging and residual risks.

INFORMATION SECURITY COORDINATION

Coordinate with IT security assurance to align testing of cybersecurity controls, share threat intelligence, and address vulnerabilities efficiently across assurance functions.

SHARED ASSURANCE REPORTING

Develop consolidated assurance reports combining findings from multiple providers, presenting a holistic risk and control status to senior management and the board.

JOINT RISK ASSURANCE MAP — COVERAGE MATRIX

Three Lines Model assurance coverage across key enterprise risk domains. Coverage levels indicate depth of assurance activities

RISK DOMAIN	1ST LINE Business Units	2ND LINE Risk Mgmt & Compliance	3RD LINE Internal Audit	EXTERNAL Ext. Audit & Regulators
Credit Risk Lending, counterparty, concentration	●	●	●	●
Market Risk Trading, FX, interest rate	●	●	●	●
Operational Risk Process, people, systems	●	●	●	●
Cyber / IT Risk Security, infrastructure, data	●	●	●	●
Regulatory / Compliance Conduct, reporting, obligations	●	●	●	●
AML / Financial Crime KYC, sanctions, fraud	●	●	●	●
Model Risk Validation, governance, output	●	●	●	●
Liquidity Risk Funding, cash flow, contingency	●	●	●	●

KEY

● Full Coverage ● Partial Coverage ● Gap / Limited ● Not Applicable

Sample for Illustration Purposes

KEY BARRIERS & CHALLENGES

What challenges or barriers, if any, limit collaboration?

1. Limited resources or competing priorities (40%)
2. Differences in objectives and perspectives (34%)
3. Absence of unified platforms such as IT systems (32%)
4. Siloed processes (31%)
5. Perceived Independence concerns (31%)
6. Skill Deficiencies (20%)

Sources: Internal Audit Foundation Risk Research Survey 2025

Risk Management Challenges in Auditing

Risk Articulation Difficulties

67% of audit findings are rejected or deprioritized by management due to vague risk descriptions (IIA, 2023). Without Cause → Event → Consequence structure, the same label means different things to different teams.

67%

of findings rejected due to vague wording

Risk-Based Decision Making

Audit plans built on last year's risk universe miss current threats. Real-time KRI dashboards, not annual heat maps, are required for evidence-based decisions.

1 yr

lag typical between risk shift and audit response

Shared Controls Testing

58% of internal audit functions report audit fatigue as a barrier to cooperation (Deloitte, 2022). Coordinated testing and shared workpapers can cut testing burden by up to 40%.

40%

reduction possible with coordination

Joint Risk Assessments

Without harmonized taxonomies and GRC platforms, the same risk appears with different ratings across IA, Risk, Compliance and External Audit — confusing the Board and Audit Committee.

90%

indicated a positive outcome from coordination between 2nd and 3rd lines

Greater Synergy between 2nd & 3rd lines

Organizations find value in coordinating risk assessment and risk management across the enterprise through improved risk coverage, reduced duplication of effort, stronger organizational alignment, more efficient reporting.

60%

synergy is possible with greater integration

Sources: IIA Global Internal Audit Survey 2023 · Deloitte State of Internal Audit 2022. Internal Audit Foundation Risk Research Survey 2025

CONCLUSION

Summary & Key Takeaways

Breaking silos is not a nice-to-have — it is a governance imperative.

01 Precise Risk Articulation

Cause → Event → Consequence is the foundation of actionable audit work. Without it, the same risk label means entirely different things to different teams — and controls miss the target.

02 Joint Risk Assessments

Siloed assessments create blind spots. A unified risk universe shared across Internal Audit, Risk, Compliance and External Audit eliminates coverage gaps and reduces duplicated effort.

03 Board-Approved Risk Appetite

Appetite must be specific, measurable, and cascaded into KRIs — not a vague statement in an annual report. For instance, zero appetite for AML; defined thresholds for credit, cyber, and strategic risk.

04 Three Lines Coordination

Assurance coordination reduces audit fatigue by up to 40%, maximises coverage, and delivers a unified risk picture to the Board. Quarterly coordination forums and shared GRC platforms are essential.

05 Real-Time Risk Intelligence

Risk-based decisions require current intelligence — not last year's heat map. Population analytics, continuous monitoring, and predictive models transform audit from 'rear-view mirror to forward-looking advisor'.

"The organisations that embrace integrated risk intelligence will be more resilient, more compliant, and better positioned to pursue strategic opportunities in an uncertain world."

RECOMMENDATIONS FOR AUDITORS

Practical actions to strengthen risk-based audit practices

01

Adopt a Risk Articulation Standard

Require all audit findings to follow the Cause → Event → Consequence structure for clarity and actionability.

02

Align Audit Universe with Risk Appetite

Continuously update audit plans to reflect changes in the organization's risk appetite, tolerance, and strategic objectives.

03

Integrate Emerging Risk Monitoring

Establish a process to identify and assess emerging risks (e.g., cyber, regulatory, geopolitical) outside normal audit cycles.

04

Strengthen Data Analytics Capabilities

Use data analytics to detect anomalies, test controls at scale, and provide real-time risk insights to management.

05

Embed Cost-Benefit Analysis

Apply cost-benefit thinking to all risk treatment recommendations to help management make informed, proportionate decisions.

06

Report Risk Trends to the Board

Provide regular risk trend reports to the Audit Committee and Board, not just point-in-time findings.

THANK YOU

Contact information

Gvantsa Gurgenidze,
CIA, CAMS_Audit, CGSS

Head of Internal Audit Function,
Bank of Georgia

E-mail: ggurgenidze@bog.ge

Social media