Asking the Right Questions in Audit

How to Provide Insight and Increase Value

Marcin Dublaszewski CIA · CGAP · CRMA

President, IIA Poland | Owner & Lead Expert, Safe ID

Audit Masters – 11th Annual Internal Audit Forum | Lisbon, 22 May 2026

Marcin Dublaszewski is President of IIA Poland (The Institute of Internal Auditors Poland) and a recognised leader in the Polish internal audit and GRC community. He brings over 20 years of professional experience in internal audit and internal control across government, local government, and commercial entities.He lectures on internal audit at postgraduate programmes at several Polish universities, and leads his own advisory practice — Audit · Training · Advisory — specialising in audit, governance, and compliance. He coordinates projects on Information Security Management System assessments under ISO 27001 and ISO 22301, and is a trainer and implementation specialist in whistleblowing systems and whistleblower protection frameworks.Marcin is a Board Member of SafeID, responsible for the sygnalistaonline.pl platform and security audits, and is an active advocate of the EU Whistleblower Directive. He holds the CIA, CGAP, AIAA and CRMA professional designations.

The audit was clean.

Seventeen findings. Clear criteria. Evidence-based conclusions.

When the audit committee asked — 'So, are we protected?' — we said yes.

Six months later, the answer turned out to be: not quite.

This is a story about what we verified, and what we never thought to ask.

Evolve or face the risk of irrelevance.

IIA Vision 2025 — The Future of Internal Audit

For decades, internal audit earned its place by answering one question: did the control operate?

That world has changed. Technology is automating the compliance layer. Boards are being asked — and are asking — forward-looking questions. Cyber threats evolve faster than annual audit cycles. ESG disclosures are being challenged in court.

The IIA put it plainly: internal audit must evolve toward strategic advisor, toward insight and foresight — or risk becoming a function that certifies the past while organisations navigate an uncertain future.

The profession responded.

The 2024 Global Internal Audit Standards redefined our purpose in four words.

Not one. Four.

ASSURANCE	ADVICE	INSIGHT	FORESIGHT
Has it worked?	*How to improve?*	*What does it mean?*	*What comes next?*

Insight means: explain what the evidence means for the objective — not just whether a control operated.

Foresight means: tell the board what might go wrong before it does, not after. Neither of those is a testing technique.

Both are questioning skills.

Our goal is not a report.

What we produce	What we intend to enable
An engagement report. Findings, criteria, conclusions. Recommendations. Management responses. A document that closes the audit.	A decision, well made. An action, taken at the right time. A risk, anticipated and avoided. An outcome that would not have been as good without us.

A clean audit report that enables a bad decision is a failure. The questions we ask determine which column we actually live in.

Strategic Advisor or Transaction Controller?

The same audit finding — two very different conversations

TRANSACTION CONTROLLER

"IT change management has a 31% exception rate against the approval policy."

"Management has agreed to remediate by Q3. A follow-up review will confirm closure."

"Overall, the function is partially effective."

STRATEGIC ADVISOR

"The control framework for change management was designed when you were releasing 60 changes per month. You are now at 200+. The framework cannot scale. This is not a compliance issue — it is a design issue."

"Before Q4, the board needs to decide: either fund a redesign, or explicitly accept materially elevated operational risk from release failures. That is a board decision, not a management one. I want to make sure it reaches you before it becomes an incident."

Then I found this.

Harvard Business Review

The Art of Asking Smarter Questions

Chevallier, Dalsace, Barsoux
HBR May–June 2024

300+ executive interviews · Delphi method · Literature review

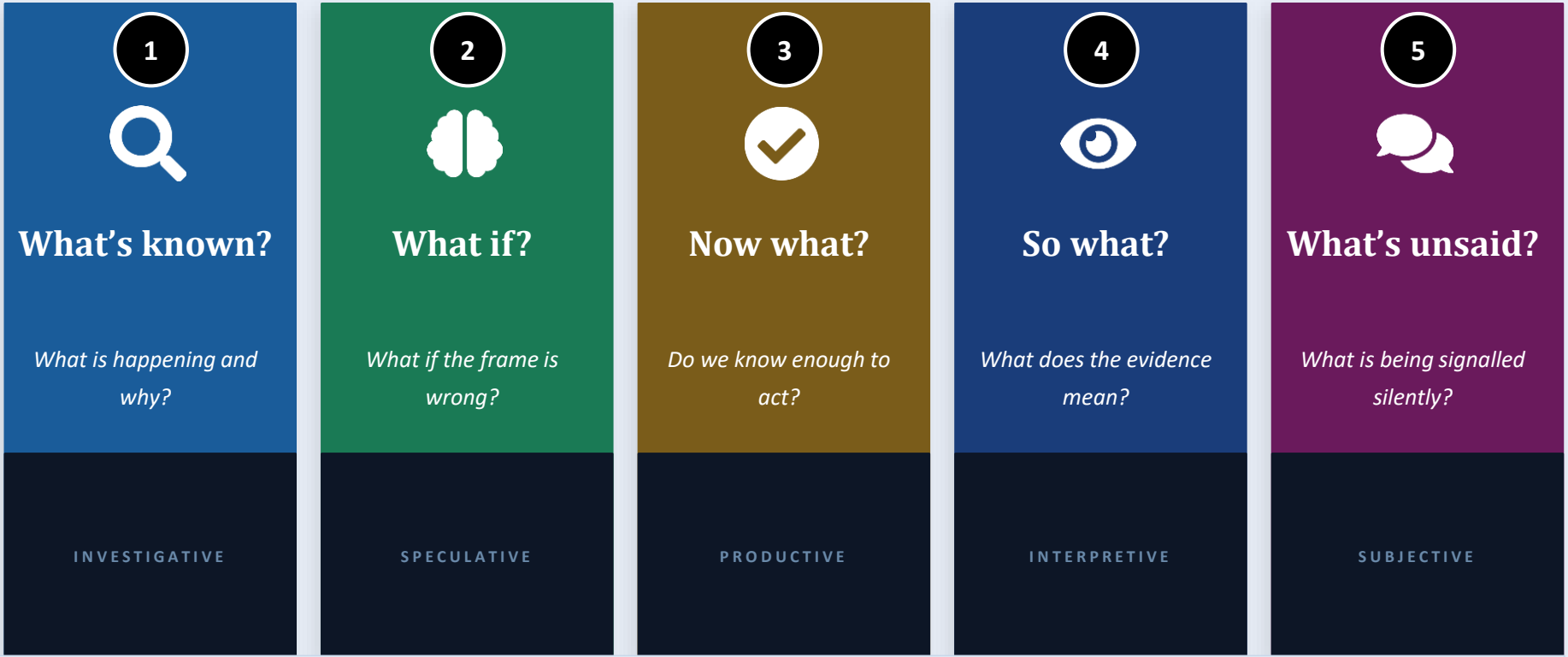
Five years of research. Three hundred senior executives. One consistent finding:

Poor decisions rarely come from bad data. They come from questions that were never asked — because the leader's habitual questioning style created blind spots they could not see from inside their own frame.

For internal audit, that landed differently. We do not just make decisions — we shape the quality of every decision our organisations make. Our questioning style is the profession's blind spot.

Five Question Domains

The Leader Question Mix — and where most audit teams leave value on the table



Most audit teams rely heavily on **1 · 3**. The biggest value gap is in **2 · 4 · 5** — Speculative, Interpretive, and Subjective.

What Each Domain Sounds Like in an Audit

Real questions — not categories

INVESTIGATIVE	*"What controls were designed to prevent this? Which ones actually operated, and where exactly did the process break?"*	Standard audit strength. The risk: auditors stop here and call it done.
SPECULATIVE	*"What if the real risk is not noncompliance but a control design that was built for last year's operating model? What future scenario would make our current conclusion wrong?"*	Opens the frame. Unlocks foresight. Most uncomfortable for auditors trained in compliance.
PRODUCTIVE	*"Is the recommended action actually feasible given current budget, staffing, and sequencing? Who owns this, and what happens if they don't?"*	Tests actionability. Prevents recommendations that are technically correct and practically useless.
INTERPRETIVE	*"So what does this mean for the objective the process was supposed to protect? Does one severe finding outweigh four minor ones? What does the board need to know?"*	Turns evidence into significance. The missing step between findings and value.
SUBJECTIVE	*"What are people in this process worried about but not saying in formal interviews? What incentive makes a workaround more attractive than compliance?"*	Surfaces organisational reality. Explains why formally correct controls fail in practice.

The moment a speculative question changes an audit.

Fieldwork interview — IT change management — Week 7

✗ **Without speculative questions:**

Auditor: "Did the change receive a valid approval?"

Manager: "31% of emergency changes used the fast-track process."

Auditor: "Noted. That is the exception rate we will report."

Finding: 31% exception rate.

Recommendation: strengthen approval controls.

Report issued. Finding closed.

✓ **Adding one speculative question:**

Auditor: "How many changes/month when this framework was designed?"

Manager: "About 60. We're at 200 now."

Auditor: "And the framework hasn't been redesigned?"

Manager: "...No, it hasn't."

Finding: control framework inadequate at current scale.

Conclusion: board decision required on framework investment.

Where Each Domain Lives

An overlay on your existing methodology — not a replacement

Planning	Fieldwork	Analysis	Reporting
Investigative	Investigative	Interpretive	Interpretive
Speculative	Subjective	Speculative	Productive
Productive			Subjective

Speculative questions before fieldwork challenge whether the scope is framed correctly. One right question here saves a week of wrong work.

Subjective questions in interviews surface what formal records and management assertions will never show.

Interpretive questions turn a list of exceptions into a business conclusion. This is where insight is created.

Subjective questions here explain why the right recommendation might still be ignored. Productive questions ensure it won't be.

In Practice: IT Change Management

What five-domain questioning changed

Context: Financial services, 200+ changes/month. Standard programme tested controls, reviewed samples, issued 17 findings. Then we asked different questions.

What standard testing found

31% of emergency changes lacked required approval.

Post-implementation review absent in 18 higher-risk cases.

One severe production outage linked to inadequate testing.

What speculative questions added

Release velocity tripled in 18 months. The control framework was designed for 60 changes per month — not 200+.

The real risk was not test quality. It was control design at scale.

What subjective questions added

Release managers confirmed informal pressure to approve within 4 hours.

The post-implementation review was widely understood as optional. Management believed the risk was low.

From Better Questions to a Defensible Conclusion

GIAS requires opinion + basis — not a list of findings

THE STRUCTURE

OPINION

Effective / Partially effective / Ineffective
in achieving the stated objective.

BASIS

Criteria used · Key findings & severity
Compensating controls · Business impact

WHY IT MATTERS

The conclusion matters because…

ACTION

Owner · Timeline · Dependencies

IT CHANGE MANAGEMENT

Opinion

IT change management is partially effective in preventing unauthorised and disruptive production changes.

Basis

31% of emergency changes bypassed approval. Post-implementation review absent in 18 higher-risk cases. One severe outage linked to inadequate testing. Control framework designed for 60 changes/month — running at 200+. Partially mitigated by strong access segregation.

Why it matters

The control design cannot provide consistent assurance at current velocity. This is a board-level decision on framework investment.

Three Conclusion Levels

What effective, partially effective, and ineffective look like in a report

EFFECTIVE

Opinion

Procurement is effective in preventing unauthorised commitments and ensuring value for money.

Basis

All sampled purchase orders approved. Competitive tendering in 94% of qualifying contracts. One isolated documentation gap — not systemic.

Why it matters

Reasonable assurance over the objective. Address the documentation gap; no systemic remediation needed.

PARTIALLY EFFECTIVE

Opinion

IT change management is partially effective in preventing unauthorised and disruptive production changes.

Basis

31% emergency change bypass. Post-implementation review absent in 18 cases. One severe outage. Control framework designed for 60/month — running at 200+.

Why it matters

The control design cannot provide consistent assurance at current velocity. Board decision required on framework redesign.

INEFFECTIVE

Opinion

Third-party due diligence is ineffective in identifying material vendor risk before contract signature.

Basis

Due diligence absent in 62% of new vendor engagements above materiality threshold. Financial stability checks absent for vendors with critical data access. Three high-risk vendors onboarded without escalation.

Why it matters

The organisation is accepting material operational and data-protection risk with no adequate control barrier at vendor selection. Immediate action required.

The executive conversation starts differently.

When we combine better questions with a defensible conclusion, the conversation with the audit committee changes. Not in tone — in structure.

Not this:

"We identified 17 findings. Three are rated high, eleven medium, three low. Management has agreed to remediate by Q3. We will follow up."

This:

"There are three things I want to make sure the board understands about IT change management before Q4. The most important is not the exception rate — it is the fact that the control framework has never been redesigned for a threefold increase in release velocity. That is a design decision that belongs at board level, not a compliance gap that belongs with management."

Where This Approach Adds Most Value

Engagements where formal compliance and real control effectiveness most often diverge

The five-domain approach is most powerful where checklists fail most visibly: complex, fast-changing, judgment-intensive areas.

Cyber & IT Risk

Speculative + Interpretive

Standard testing verifies patching and access controls. Speculative questions surface what the threat actor sees that the risk register doesn't. Interpretive questions connect findings to business disruption, not just control status.

What would a sophisticated threat actor see in our control landscape that we are not seeing ourselves?

Transformation Programmes

Speculative + Subjective + Productive

PMO compliance audits check schedule and budget. They rarely ask whether the target state control environment is being designed adequately. Subjective questions surface whether implementation teams are signalling distress.

Are the people closest to this programme confident that the controls will work when we go live?

ESG & Non-Financial Risk

Speculative + Subjective

Data integrity checks are investigative. Speculative questions test whether disclosures reflect actual practice or aspirational targets. Subjective questions surface the organisational pressures that make ESG data drift from reality.

What pressure exists in this organisation to make ESG data look better than it actually is?

Better questions. More useful audit.

Before scoping — Speculative questions challenge whether the objective is framed correctly. One right question here saves a week of wrong fieldwork.

During interviews — Plan subjective questions in advance. The most important insights in an audit rarely arrive uninvited.

Before issuing — Ask: which domain is underused? If interpretive is weak, the report will not explain what the evidence means. Fix that before it goes out.

Our goal is not a report. Our goal is a decision well made — and these questions are how we get there.

Your turn.

A few minutes — with the person next to you first, then share with the room

Q1	Which of the five domains does your function overuse — and which do you most often neglect? Think of a specific engagement.
Q2	Think of a recommendation that was logically correct but barely implemented. Which domain was probably missing?
Q3	What would it take — in methodology, culture, or your relationship with management — for your team to use subjective questions more confidently?
Q4	What is the one thing that would most change the quality of the conversation between your function and the board?

Before your next report:

ask which question domain is missing.

That one question — asked honestly, one minute before every report goes out —

will tell you whether you are delivering assurance, or whether you are also delivering insight and foresight.

Our goal is not a report. Our goal is a decision well made.

Thank You.

Let's discuss.

Audit Masters – 11th Annual Internal Audit Forum | Lisbon, 22 May 2026

Marcin Dublaszewski

CIA · CGAP · CRMA

President, IIA Poland
Board Member SafeID
CEO Audit Training Advisory

"Transform or become irrelevant."
— IIA Vision 2035