Navigating Internal Audit Opinions and Ratings in Today's High-Stakes Environment

In an era where regulatory scrutiny and reputational stakes are intensifying and audit committees demand greater assurance, internal audit (IA) functions face mounting pressure to deliver clear, actionable insights. Behind this lies a seemingly straightforward question that quickly reveals layers of complexity: how should we rate and communicate audit findings?

The Strategic Importance of Audit Ratings

Internal audit ratings serve as the primary language through which complex assessments are distilled for senior management, boards, and regulators. These ratings (evaluation systems that categorize the severity of findings) often determine how governance, risk, and compliance (GRC) issues are prioritized and addressed across the organization. Yet despite their critical importance, there remains considerable variation in how organizations approach their rating methodologies.

"The rating you assign doesn't just communicate the current state—it can shape future action," notes Stephen Foster, former CAE (Chief Audit Executive). "It's the difference between an issue being treated as a key threat requiring immediate senior management involvement rather than a minor operational hiccup to be handled by line management."

Alignment with Enterprise Risk Management: Opportunities and Pitfalls

Some organizations gravitate toward aligning their audit ratings with existing enterprise risk management (ERM) frameworks—typically focusing on impact and likelihood assessments. This approach offers several distinct advantages:

- **Common Language**: It creates a unified risk vocabulary across the organization
- **Familiarity**: Key stakeholders already understand the framework
- **Integration**: Audit findings can seamlessly feed into broader risk management processes

However, this alignment can carry risks that audit professionals must consider. Standard ERM frameworks often struggle to capture the subtle nature of certain emerging risk categories like ESG (Environmental, Social, and Governance), cybersecurity best practices, DORA and risk culture. Additionally, existing frameworks may have inherent limitations in how they rank and assess the impact of risks (e.g., reasonable worst case impact or something else? And how do we judge likelihood?) alongside the effectiveness of controls versus the residual risk exposure.

The Aggregation Challenge

Another dilemma faces audit professionals when an assignment encompasses multiple areas or processes. Should ratings be:

1. Combined to provide a single overall assessment?
2. Reported separately for each distinct area?
3. Ranked and then combined with an overall rating supported by component ratings?

Each approach presents trade-offs. Combined ratings offer simplicity but risk obscuring important 'cracks' in specific areas. Separate ratings preserve detail but can create report fragmentation. Ranking approaches can offer the best of both worlds but can demand sophisticated methodology and can create confusion if the relationship between rating levels isn't clearly articulated.

Evidence Base and Rating Confidence

The depth and breadth of audit work significantly impacts rating credibility. Limited-scope reviews, advisory engagements, and continuous monitoring activities on narrow areas present challenges when determining appropriate rating methodologies (e.g. you may look at a control/process area through analytics but miss IT General Controls/Access questions.

A crucial distinction exists between ratings based on comprehensive evidence versus those derived from more limited sampling. When resource constraints necessitate narrower scope, how should this impact:

- The rating terminology used

- Confidence levels expressed

- Limitations explicitly acknowledged

Progressive audit functions have developed innovative approaches to this challenge, including:

- Confidence-scaled ratings (e.g., "Medium risk with low confidence")

- Explicit scope limitations attached to ratings

- Tiered rating systems based on engagement depth (e.g., no substantial assurance when work is limited)

Balancing Positive and Negative Elements

Some audit functions rate areas based on the absence or presence of deficiencies and control gaps. However, other internal audit functions recognize the importance of balanced assessments that reflect strengths alongside weaknesses.

Some organizations have adopted "dual-factor" rating systems that separately assess the control environment (or risk culture) maturity and the residual risk exposure. Others incorporate "positive assurance" language alongside traditional findings with behavioural risk questions being increasingly considered where it matters.

When Management Becomes 'Comfortably Numb' to Ratings or Starts to Over-react to Bad News

Another risk in audit rating systems can arise when "satisfactory" ratings become the default expectation rather than a meaningful assessment of good (or excellent) practice in risk control. When this occurs, there are three significant risks:

1. **Management Complacency**: When top ratings become easily achievable, continuous improvement incentives diminish

2. **Credibility Loss**: When significant failures occur in supposed "well-controlled" areas, internal audit's standing suffers.

3. **Over-reactions to Negative Ratings**: This can create a fear or blame dynamic in the organisation

Conversely, excessively stringent rating approaches that make top ratings hard to achieve create different problems— e.g., stakeholder frustration and management seeking a different risk appetite. However, there are techniques that can help get the best of both worlds.

Building for the Future

Forward-thinking audit functions are exploring:

- Multi-dimensional rating frameworks that separately evaluate design effectiveness, operating effectiveness, and target vs. actual risk exposure.

- Dynamic rating systems that incorporate trend analysis as well as potential future vulnerabilities.

- Ratings that consider best practices and root causes (as now required by the GIAS - Global Internal Audit Standards) and consider how the new GIAS 'topical requirements' will be factored in.

- Technology-enabled approaches that leverage data analytics, process visualisation and AI to provide more objective and impactful ratings

Finding Your Path Forward

There is no one-size-fits-all solution to the rating conundrum. Each internal audit function and organisation must consider its risk context, stakeholder expectations and risk culture when designing or refining its approach.

Key questions to consider include:

- How do our current ratings align with stakeholder expectations and organizational objectives?

- What evidence supports the effectiveness of our current approach and where could there be gaps?

- What unintended behavioural consequences might your current rating approach create?

- How are behavioural, cultural and best practice GRC elements considered?

- How well do audit ratings drive appropriate action and prioritization?

- What is the evidence trail that underpins any ‘overall opinion” from internal audit?

By thoughtfully examining these questions and considering the diverse approaches available, internal audit functions can develop rating methodologies that drive meaningful organizational improvement while providing appropriate “reasonable” assurance.

As regulatory environments continue to evolve and board expectations intensify, the strategic importance of well-designed audit rating systems will only increase. The organizations that thrive will be those whose internal audit functions can communicate complex findings through rating frameworks that balance simplicity with nuance, consistency with flexibility, and detail with clarity.

Join the upcoming webinar to explore this topic further.