Key Takeaways from NeuGroup's 2019 H1 Internal Auditors' Peer Group Meeting

NeuGroup Insights

IAPG members discuss taking a more rounded approach to assessing risk, managing execs from afar, IA budget sensitivities, reducing audit cycle times and third-party audits at its first-half meeting.

Sometimes Precision Works Against You

Too much precision can muddle the early stages of assessing risk.

When pursuing the first steps to assess risk, risk professionals may want to look past their desire to employ precise information and start instead with ballpark estimates.

"As you get more precise, the culture of some companies or groups within companies will tend to get into debates about whether a precise risk measurement is right or wrong," said a member of the Internal Auditors' Peer Group (IAPG) at a recent meeting. "To avoid going in that direction, we try to simplify."

He said that internal audit did some "betas with more precise elements … and found a ton of debate." He added that his Fortune 500 company, with a high concentration of strongly opinionated "super-alpha types," may be especially prone to such back-and-forth.

"So as I went down that rabbit hole with [this initiative], I realized it wasn't going to work, and that simplifying [the information] was the only way to survive the exercise," he said.

How to avoid debate. Essentially that meant removing any measurement of risk from the discussion. Instead, his group asks the key players about the potential or likely impact of risks—"We call it ballparking, or ERM light," he said. "A very simplified approach to get them" to avoid having a debate.

The precision issue arose in an IAPG session devoted to how integrated risk management (IRM) improves decision-making and performance through an integrated view of how a company manages its unique risks, and how that gels with internal audit (IA).

One approach to ERM. The member said that instead of analyzing multiple possible risks, his group begins the risk assessment process at elements important to the company's business strategy, followed by the likelihood of process and control concerns. In the first phase, IA has created a framework reflecting the company's four business-process flows, which it arranges according to their business-strategy importance and the likelihood of process or control concerns.

"So as people assess [the framework], they're able to say, 'I have knowledge of this flow or I don't, and so I'll respond or not,'" he said, adding that IA collects this information via surveys and one-on-one meetings with senior management.

The second phase explores the top five risks the executive team should focus on, and those themes typically map to the process-centric framework developed in the first phase. IA can then align each risk to its executive sponsor and subsequent sponsors, enabling the creation of a slide that illustrates the top five risks and how management mitigates them.

IA then asks for management's views to fine-tune the process. Exact measurements are not a part of the discussion, and instead IA seeks to guide them to "common-sense" conclusions and obtain their validations before approaching the board of trustees.

"It's a relatively simple model that doesn't quantify a bunch of things, and the feedback we've gotten from all the external directors joining the board is that they like the process. It's not too complicated and makes sense to them," the member said.

He noted that when Standard & Poor's introduced risk management as a debt-rating factor several years ago, his company's general counsel brought in a third party to provide an alternative risk assessment. Its approach sought more precision to arrive at the risk assessments, but management

disputed the Big Four firm's conclusions and there was " a complete uproar," he said.

"There's a ton of value to precision, but you have to gauge what fits your company's culture," the member said.

Managing Execs from Afar

Managing IA execs who are far away from HQ creates problems.

As multinationals spread their businesses across the globe, internal audit (IA) must follow. But does that mean lots of long plane flights or can IA executives be stationed overseas if no manager is present?

That question was asked at NeuGroup's recent Internal Auditors' Peer Group meeting.

"I'm curious about whether people with [IA] resources in other countries and no manager there have found that resulting in issues or if it works fine," said one member, who said that she would like to add a few more positions in India to her team. She added that she inherited two IA executives stationed in China with no manager, and while the arrangement is working, they seem a bit isolated.

Another member noted that the first of three IA staff her company hired in India was a manager, in part to help with additional hires, but the plan was to have such a manager in country.

It can work. If it's only a few people in the country, said another, then they should be senior employees who are independent and have enough experience to get things done in the country. But keeping them part of a cohesive team remains difficult, even if you bring them back to US headquarters regularly. He noted having a few senior IA staff in Canada, but said it was still better to have someone managing them, even if from afar.

And as a rule of thumb, another member said, the staff in an overseas office should be at least three strong, since having one is "a never, and two is borderline because if one person leaves you're back down to one."

Management isn't the only issue. Several members agreed that a local lead or manager is helpful to keep the team cohesive and motivated, since that can be difficult to do from across the ocean. And managing them isn't the only issue, pointed out another participant, since managing them from afar means their manager won't know them as well as those he or she is in contact with frequently and so will have to rely more heavily on data to assess their performance.

"I've wondered whether these people are even getting a fair shake, since no one knows them as well," she said. "I think there are a lot of elements to it on the people-management side."

IA Budget Presents a Gentle Balancing Act

Internal audit budgets can often prove tricky; finding the Goldilocks amount.

Determining the budget for internal audit (IA) is a balancing act—too little resulting in lawsuits, too much in audit fatigue—that is best achieved through transparency about the most assurance funding can buy.

The Internal Auditors' Peer Group (IAPG) wrapped up a recent meeting by discussing how to address a question from the board of directors' audit committee about whether IA's budget is sufficient. Like other corporate support functions, IA is typically competing for a slice of the company's overall budget, but audits can also go overboard.

"If you're out grinding this stuff too much, you can bring [corporate functions to their] knees" by over-auditing, one participant noted.

One approach. Another participant described an approach that others said echoed their own. When this member joined his company several years earlier, the CFO asked him about the state of IA's budget. He asked to lead the enterprise risk process, which he did over the next few months, to "put down a baseline." From there, his team drew up an audit plan that provided "minimum, ideal and maximum" audit scenarios based on the determined risks, and the level of risk coverage according to board expectations.

From there, he could determine the total audit hours necessary, how many full-time equivalents (FTEs) would be necessary to complete the work, and their estimated compensation.

"Here's the total budget and does that make sense?" he said. "Again, we established a baseline and worked off that."

He noted that taking that approach still involves haggling—IA may request $2.7 million, the audit committee asks if $2.2 million would work, and they agree on $2.5 million. "It boils down to what we're given to work with. As long as the quality of the assurance we're giving the board remains, we should be fine," he said.

Why transparency is important. Another member described internal audit as similar to health insurance: "You don't know how much you need until you're sick" but "are you going to have a shareholder lawsuit if you don't invest enough" in IA.

The consensus of most IAPG members appeared to be that providing the audit committee with as much transparency as possible about what they'll get for their money in terms of auditing is the most effective approach: essentially putting the ball in the audit committee's court. One member shared a situation in which the audit committee noted IA's important findings and asked what would happen if its budget was doubled.

"I'm like, if this is what you want, you're welcome to it, but there's also audit fatigue and you can bring [functions] to their knees," the auditor said, adding that IA will execute whatever is asked of it, whether it's to oversee a change in regulations, GDPR, or something else. "We'll make thoughtful recommendations and, if necessary, step things up for more resources. But it's a gentle balance, and that's the hard part."

Tips for Reducing Audit Cycle Time

Former IAPG member Michelle DeBella shares cycle time tips; simplify and don't fear escalation.

The longer it takes to complete an audit, the less impact it is likely to have, especially for new and rapidly growing companies, prompting internal audit's struggle to reduce the audit cycle time.

Michelle DeBella addressed that issue at a recent IAPG meeting, borrowing from her experience running internal audit (IA) at Uber, and earlier for a long stint at Hewlett Packard Enterprise and HP Inc. (HP).

"We invest a lot of our time and talent in audits, and if we don't get audit results in a timely fashion, their impact can be lost," Ms. DeBella said. "Really dynamic companies don't want audit results as a scorecard of what they did, but to show them what they can work on and where the risks lie. And they need that information in a timely fashion to put into their budget and planning processes."

Shorter is better. Long audits can drain the audit team's sense of engagement and excitement about what they're doing and its focus, and they tend to be inefficient, wasting already limited resources, Ms. DeBella said. She then provided "process accelerator" tips on the "how" and "what" to audit. Changing how to audit is "low-hanging fruit," she said, but also challenging because people are used to the existing approach.

Simplicity is key. At Uber, her team standardized the audit scoping and planning form, making it easy to fill out and as multipurpose as possible by minimizing the narrative and instead providing boxes to check and/or simple-text entry. She said she also supports standardizing and simplifying the audit report.

"I believe if you put word on paper, somebody must review it. So every additional word adds to cycle time," Ms. DeBella said. She added that in a global company where English is not everyone's first language, a highly narrative report can be difficult to understand or even produce, slowing the process and reducing the impact. Plus, fewer words mean fewer errors and less time-consuming wordsmithing by stakeholders.

"You can pursue audit reports that have the same look and feel, but you can make them relevant to stakeholders in very different areas: legal, technology, accounting, engineering, etc.," she said.

At rapidly growing Uber, her team agreed to keep the audit report very simple: a one-page executive summary and one page of metrics to help convey the size and scale of the

business. To avoid delays from an issue owner inquiring about an issue, detailed issue information and testing attributes were captured on a separate form. Simplifying the report template, she said, also reduces variability and the need for chief audit executive (CAE) review of the full report.

Ongoing remediation. Ms. DeBella added that her HP team sought to dispel the notion that remediation can only occur after the audit, sometimes resulting in a "gotcha" scenario whether intended or not. Instead, Ms. DeBella said, it is more efficient for IA to offer results as the audits progresses, enabling management to implement remediation plans along the way.

Rely on IA staff. Most participants in the IAPG meeting acknowledged reviewing every report, but that can slow the process. Ms. DeBella said that, based on risk, she removes herself from certain review cycles, such as reports for audits with few issues, and instead relies on her directors to put out quality reports.

Enforce SLAs. Tough service-level agreements (SLAs), handled politely, can also speed up the audit process. Ms. DeBella's team first sets deadlines for themselves, requiring audit report drafts to be completed for manager review by specific dates. To drive accountability, late audit-report delivery is captured by a metric that also reveals who held up the process.

The IA team crafted a similar SLA for the business owners, giving them 48 hours before audit-report publication to comment, ask questions, and/or clarify incorrect text. Emphasizing factual correctness countered stakeholders' attempts to wordsmith. "The more transparent we were upfront about SLA times and sticking to them, and explicit about what those 48 hours were for, the better it worked," Ms. DeBella said, noting the importance of refreshing that message in a professional manner at the start and close of the audit.

Don't fear escalation. "Teams don't have to feel bad about asking, 'Do you have any comments? We're going to publish tomorrow'—that's not a mean message," Ms. DeBella said. She added that if management stubbornly misses deadlines, emphasizing that late-response metrics will be reported to the audit committee is an effective tactic. "At HP, we were highly focused on that statistic, and there was a concerted effort by management not to show up on that list," Ms. DeBella said.

Support from above. Ms. DeBella said Meg Whitman, the HP CEO she served under, supported escalating issues in 24 hours and resolving them in 48. Resolving complex audit issues in that time may be rare, but a culture where timely issue resolution is expected creates the right kind of pressure to drive action. And if stakeholders argued that signoff from another department's president was necessary, Ms. DeBella reminded them of the deadline and gave them options to pursue commitments from lower-level executives.

What to audit. Bringing representatives from each corporate function as well as management to the audit-planning table can also reduce cycle time by decreasing the likelihood of loose ends or the need to bolt on an overlooked element. Plus, it can help determine whether it makes sense to perform a lengthy big picture audit or deliver smaller pieces of information more rapidly. That is especially true for fast-growing companies, Ms. DeBella said, where immature processes under audit may change even before a major audit is completed. "Some of that [planning] will drive audit speed, too, because you don't end up auditing things where change is already in progress or that don't add value," she said.

Audit intensity can vary. For example, Ms. DeBella said, her team found that self-assessments were more appropriate in low-risk countries or well-defined lower-risk processes. So internal audit may have three or four audit plans of different size and intensity that fit the different situations. "Some audits can be executed very fast, and the end-to-end audit can be saved for something that has a bigger pile of risks associated with it, or management wants a deeper view of," Ms. DeBella said. "Not every audit has to look and feel the same."

Good practice. In fact, smaller, tailored audits can benefit staff development, Ms. DeBella said, enabling the audit team to practice interview and documentation skills as well as sizing up risk and negotiating their findings with stakeholders. "There are so many benefits from those small and manageable projects," Ms. DeBella said.

Third Parties Can Be Supply Chain Party Poopers

Auditing third parties: Black-swan risk and supply chains.

Potentially crippling risks can come from just about anywhere, but third parties, especially those in the supply chain, can be particularly problematic and so critical for internal audit to find ways to review.

"From an [enterprise risk management] standpoint, how many of us do a black-swan analysis and really think the unthinkable?" asked a member of the IAPG at a recent meeting.

After a tepid response from other members, he said he had completed such an analysis for the first time at the start of the year and presented the results to the company's board of directors.

A focus of the analysis was third parties, especially in the company's supply chain, since the failure of such a third party could bring the IA's company "to its knees." The member added that such an analysis helps IA hone in on which types or categories of third parties, or even which specific third parties are the ones to focus on in terms of rare but impactful black-swan risk.

"The whole thinking about the knock-on effect, if you will, and how it would reach my shores is super-critical to understand to evaluate that risk," he said.

Another member asked how to facilitate such analysis, since if he "knew the unknown it would already be on the chart." The first member noted a "shadow committee" at his company that's subordinate to a board-level risk committee that's part of the ERM process and meets at least once a quarter to bat around ideas about what could go drastically wrong. That shadow committee comprises the heads of human resources, finance and legal, as well as the COO, to lesser extent the CEO, and selected deputies from their teams.

"Can a satellite fall out of the sky? An engineer will say 'yes,' so what would that do to our stock price?" he said. "Taking that kind of thinking and it becomes very clear to everybody that the core value chain of the company is what you're trying to protect, and supply chain is a key component of that value chain."

He added that the analysis prompted focusing on Amazon Web Services, since "if something goes wrong with this beast, then we're pretty much dead in that water."

Another member noted that such a level of black-swan scrutiny was less appropriate for high-growth businesses, where risk acceptance and tolerance are much higher.

"You can't really think of everything that could possibly go wrong, because then you wouldn't do anything," he said, adding, "The nature of your activities also helps determine how in-depth an exercise you want to do about black-swan type risks. If I did that in my world and presented to the board, my CEO would smack me over the head and ask why I was wasting my resources."

Some group members concluded that the level of black-swan scrutiny should increase with the maturity of a company, especially if it is reliant on government contracts that could be jeopardized should a black-swan event result in noncompliance.

The first member agreed that IA must ensure management is onboard with pursuing such analysis and making sure the issue, while unlikely to happen, is nevertheless "relatable"—more achievable if management's "lieutenants in the field" identify a black-swan-type risk. For example, they may point to a member of a rapidly growing company's supply chain that has become excessively critical—too many eggs in one basket.

"So it's incumbent for us to do something about it, to recognize it, and to not wait for us to come crashing down before we do something about it," he said.