INTERNAL AUDIT HOT TOPICS - PITFALLS AND HOW TO AVOID THEM

AUTHOR: KIRSTY MARTIN

It's internal audit program planning season! As internal audit consultants we get the opportunity to work with a variety of diverse organisations auditing a wide range of different topics. This gives us unique insight into trending topics and common issues that might be worth considering for your organisation.

If you're working in the public sector, it will probably come as no surprise to you that areas like integrity, climate change risk management, third party risk management, information management, artificial intelligence, and conflicts of interest are finding their way onto a lot of audit programs – and for good reason. These are areas of emerging risk and increasing public scrutiny that are timely to seek some assurance confidence over. Here we outline some the common pitfalls that are worth considering when auditing these trending topics and how to avoid them.

Integrity

Across the broader Australian Public Service (APS), there has been a marked increase in the attention and emphasis directed toward the concept of integrity. This focus was initially driven by the Independent Review of the APS (the 'Thodey Review') in 2018 and is central to the current APS reform agenda which includes a priority area focused on promoting "an APS that embodies integrity in everything it does".

Everyone knows that integrity is a hot topic, but the main pitfall we see is simply uncertainty about how to actually embed it, and even more uncertainty about how to provide assurance over it. For agencies that have started to dip their toe in the water of auditing integrity, the initial focus tends to be on assessing whether good policies/procedures/training etc. are in place – i.e. – "are we **saying** the right things?". This is an important place to start, but the real challenge comes in understanding whether people are **doing** the right things and acting with integrity in practice.

Starting small with a relatively high-level framework-based review will still deliver value. Auditing integrity in any way helps to demonstrate that it is an organisational priority and will start to get people thinking about what it means to be held to account for an integrity culture. To get the most value out of this type of review, it is important

to consider how well messaging is tailored to the actual organisational context (and the different contexts within the organisation) to support staff to understand integrity as an everyday consideration rather than an abstract concept.

But to start to get assurance over the integrity culture in practice, auditors need to consider broader techniques such as surveys, staff interviews, focus groups, behavioural observation, and business context analysis. This too can start relatively high level to get initial insights and inform future planning for more targeting reviews. Where integrity culture is a high priority and higher assurance confidence is desired, a more robust and repeatable program of integrity culture audit can be developed. To get value from these more comprehensive audits, it is crucial to define and agree what a good integrity culture looks like for that organisation, including key desirable and undesirable behaviours, to provide a consistent baseline against which to compare.

Climate Change Risk Management

The introduction of climate disclosure reporting requirements for Commonwealth entities has boosted climate change risk management up the agenda from an assurance perspective. The main pitfall we've noticed in this case is a focus purely on ensuring preparedness for compliance with the new requirements. Although this is important, internal audit functions should take this opportunity while climate risks are front of mind to promote and explore other aspects of climate risk management that are important organisational considerations.

Depending on the nature of the organisation, additional aspects that should be considered include how climate risks may impact Work Health and Safety, Business Continuity Planning, and Disaster Recovery Planning. **Have these policies and the associated risks and controls been re-assessed in light of a changing climate and more regular extreme weather events?** Does the organisation have clear rules and guidance in place around things like extreme heat and are these understood and implemented in practice?

More broadly, have climate change risks been considered strategically where they may have a direct impact on agency goals? Have these risks been factored in as part of development of strategies and goals, and are they considered on an ongoing basis? The nature of these risks will vary greatly between organisations, but there are potential impacts to consider across health and social outcomes, infrastructure, productivity, service delivery and more that will be relevant for various public sector agencies.

In considering climate change related risks, specific expertise is generally required to ensure an audit is sufficiently robust to provide more than surface level insights. Such expertise supports the audit team to more effectively challenge management assumptions were needed and ensure risks are fully understood and nothing is missed. For this reason, including a subject matter expert as part of the audit team is crucial to ensuring value.

Third-Party Risk

Outsourcing, shared services, and reliance on third-party providers are now entrenched features of federal government operations. Whether it's IT infrastructure, defence procurement, health services, or consulting engagements, third parties are often integral to delivering core functions. However, although you can outsource services, **you cannot outsource risk**.

The key pitfall we come across in auditing third-party risk is confusion around the concept itself and who is actually accountable and how these risks can and should be managed. Unfortunately for the public sector, the public don't much care for excuses. Even if the issue was 100% the fault of the third party – how could the government have allowed this to happen? Why weren't you monitoring it? Why didn't you do your due diligence? **Again, you cannot outsource your risk**.

Third-party risk is multifaceted - spanning performance, cyber security, ethical conduct, compliance, data privacy, and financial integrity. Failures by external partners can have significant consequences for service delivery and public confidence.

As a result, internal audit must ensure that third-party governance frameworks are robust, including due diligence processes, contract management practices, and monitoring mechanisms. This also extends to sub-contractors, where transparency and accountability may be further diluted. Third-party risk is a crucial topic to audit to help agencies understand their risk profiles and identify improvement opportunities. Auditors can add further value by treating stakeholder engagement throughout the audit process as an opportunity to educate on accountabilities and expectations to support improved understanding and risk culture as this capability gap tends to be the main barrier to strong third-party risk management.

Information Management

Information is one of the most valuable assets in the modern public sector. Information management refers to the creation, description, preservation, storage, protection, usage, disposal, and governance of digital and non-digital records and data that are relevant to the operation of an entity. Good information management maximises the value of an agency's information assets by ensuring they can be found, used and shared to meet government and community needs and support the efficient and effective delivery of outcomes.

This is relatively well understood across the public sector, and as a result, information management is a regular feature on audit programs. There are plenty of useful and detailed standards that can be applied such as the Information Management Standard for Australian Government which align to obligations under the Privacy Act and Archives Act that make for a relatively straightforward audit. But there is one crucial element that these "straight forward" information management audits ignore – people.

In our experience, the biggest risks from an information management perspective are not systems, but people. We've seen agencies with world class systems and processes and well-tested system controls – where staff save everything offline on their desktop and make endless use of workarounds to avoid ever having to touch that world class system. This human side of information management is crucial to consider in the design and delivery of an information management audit to get a true understanding of risk levels and effectiveness.

Conflicts of Interest

Conflicts of interest, whether real or apparent, can undermine the credibility of government decisions. In a public sector context, where impartiality is paramount, even the perception of bias or favouritism can erode trust. From procurement panels to grant allocations and recruitment decisions, conflict of interest risks can be found across everyday government operations. Recent scrutiny around conflicts of interest in the public sector has pushed COI onto the agenda for many audit committees.

There are some common pitfalls we have noticed that should be considered when scoping an internal audit. Most agencies have a decent COI Policy, with COI built into annual training programs – but this is really the bare minimum. Implementation and truly embedding understanding of COI into business as usual is where it tends to come unstuck.

For example, it is worth remembering that the relevant requirements under the Public Governance Performance and Accountability (PGPA) Act, and PGPA Rule are mostly **not framed around *conflicts* of interest, but rather disclosure of *any material personal interests***. The intent is to manage real or apparent conflicts – but a lot of agencies seem to place such a focus on conflicts that they forget that disclosure requirements relate more broadly to any material personal interests.

As a result, material personal interests tend to only be considered in individual contexts in case there is a potential conflict there. Disclosure processes are often completely disjointed or siloed with no central repository or visibility across the organisation. But the people making the disclosures don't always know that and often assume if they have disclosed an interest in one place for one purpose, then they have ticked off on their duty.

In auditing conflicts of interest management, particular attention should be paid to whether/how personal interest declarations are managed holistically. Additionally, it is very difficult to audit whether appropriate interests have been declared – as auditors simply don't know what they don't know. We can audit whether declarations that have been made have followed appropriate processes, but what about declarations that weren't made? An element of culture-based audit utilising techniques like surveys or interviews can be useful to provide additional insight on this aspect.

Artificial Intelligence

AI is the word on everyone's lips as the power and prevalence of the technology continues to expand. In the public sector, there are rightly concerns around how and when AI can or should be used while maintaining integrity, protecting privacy, and meeting community expectations and legislative obligations (noting that most program legislation was not drafted to cater for AI). However, most agencies are already using AI in some capacity and planning to increase usage. As a result, audits of AI governance are popping up as a high priority.

Drawing on recently released whole-of-government guidance like the Australian Government Policy for the responsible use of AI in government and the Australian Government AI Assurance Framework, audits tend to focus on agency policies and governance arrangements for the design, development, deployment, monitoring and evaluation of agreed use cases.

Although this is of course crucial, a key element that is not always captured or considered are the **unapproved use cases that the agency might not even be aware of** as staff look for ways to increase efficiency in their day-to-day workflows using publicly available tools. Internal Audits of AI governance should include consideration of broader AI culture across an agency and how risks around "shadow AI" from unauthorised individual use cases are understood and mitigated.

CONSULTANCY THAT VALUES BIG THINKERS, WHO SOLVE UNIQUE PROBLEMS.

CONTACT US:

Mark.Harrison@sentcon.com.au
0408 661 325

Josie.Lopez@sentcon.com.au
0417 464 283