

nts SPEECH

Strategic governance of risk: Lessons learnt from public sector audit

PUBLISHED Wednesday 8 August 2018

Contact

Please direct enquiries through our [contact page](#).

Grant Hehir, Auditor-General for Australia, attended the Institute of Internal Auditors-Australia 'Public Sector Internal Audit Conference' on 31 July 2018, and presented an opening keynote session titled *Strategic governance of risk: Lessons learnt from public sector audit*. The accompanying paper to the speech, which was delivered against a conference theme of 'internal auditor as a trusted advisor', is available [here](#).

Introduction

The importance of effective risk management has been highlighted in many reviews of organisational failure. Most recently, in the private sector by the April 2018 Australian Prudential Regulation Authority (APRA) *Prudential Inquiry into the Commonwealth Bank of Australia* and prior to that, in the public sector in Professor Peter Shergold's August 2015 report, *Learning from Failure: why large government policy initiatives have gone so badly wrong in the past and how the chances of success in the future can be improved*. These reviews have focussed on the importance of not just having good risk

processes, but also strong governance and clear accountability to establish effective risk culture. Not surprisingly, some Auditor-General reports have similar findings. This work suggests some key indicators of an effective risk culture, including:

- the board and its sub-committees engaging with risk through establishing risk appetite and tolerance, along with active oversight and challenge of management responses to emerging risks;
- clear responsibilities and accountabilities for risk and an effective performance framework linked to risk outcomes;
- monitoring implementation of risk treatments, changes in risk ratings, and emerging risks;
- proactive, not just reactive, approaches to risk;
- learning from your own and others' mistakes;
- fit-for-purpose management arrangements, which are consistently communicated; and
- adequate resourcing with a focus on building staff capability.

This paper will consider the lessons underlying these indicators through an analysis of the APRA inquiry, Dr Peter Shergold's *Learning from Failure* and a number of Auditor-General reports.

Why an effective risk culture is important

Positive risk culture means improved accountability, governance, performance, resilience and financial management. Effective risk management is core because of how it drives strategic and operational planning.

Improved outcomes

Good risk managers, supported by organisations with positive risk culture, prevent or reduce failure, resulting in improved outcomes. Positive risk culture is also an enabler of innovation. If staff are afraid to fail, they are unlikely to take calculated risks and be

innovative. If an organisation is unclear about its risk tolerance, it cannot expect innovation. Good risk managers produce innovative outcomes, because their entity's risk tolerance allows for failure, remediation and learning where the decision making in the risk management process was sound.

Identify and manage threats, and capitalise on opportunity

Organisations with positive risk culture can more easily and more quickly identify, evaluate and manage threats and opportunities. A positive risk culture will result in staff who are vigilant, regularly monitoring and documenting the implementation of risk treatments, changes in risk ratings and emerging risks. Entities with positive risk culture foster confident staff who raise suggestions relating to new or identified risks. The APRA prudential inquiry noted that one indicator of sound risk culture is when information on risk flows freely without fear of blame. Positive risk culture means decreased potential for unacceptable or undesirable behaviours such as fraud and harassment.

Productivity and efficiency

An organisation with positive risk culture identifies risks more quickly, resulting in more agile management. Decision making is better informed, and staff feel empowered to make difficult decisions, reducing time lost to indecision. These factors will generate productivity and efficiency.

Consequences of ineffective risk culture

The consequences of poor risk culture are damaging. Something observed in the Commonwealth Bank by APRA was wide spread complacency, which APRA suggests bred over-confidence and a lack of appreciation for non-financial risks. The Home Insulation Program is an example of a particularly poor outcome. Auditor-General's Report No. 12 of 2010–11 *Home Insulation Program* assessed key aspects of the

establishment and administration of Home Insulation Program by the Department of the Environment, Water, Heritage and the Arts, as well as the transition of the program to the Department of Climate Change and Energy Efficiency. This audit report found that there were a number of contributing factors that impacted on the success of the program, one of which was underestimation of key program risks. As a key learning, that audit noted that a clear understanding and acceptance of the level of inherent risk and potential consequences of realised risks in the program by all key stakeholders, including government, can avoid reactive program changes following implementation. This approach requires realistic and accurate reporting of circumstances by departments and agencies to key stakeholders.

What positive risk culture looks like

Positive risk culture is where risk appetites and tolerances are clearly defined and communicated, in an environment where staff have the capabilities to deliver risk management that is consistent with those appetites and tolerances. Entities with positive risk culture effectively identify, assess, monitor and manage risk across all levels, identify risks before they are realised, and focus on the lessons to be learnt when risk management doesn't achieve the desired results.

In the Department of Finance's *Benchmarking Survey 2017 – Risk Management Capability Maturity Levels*, 'optimal' risk culture is where 'the culture of the entity is one that demonstrates and promotes an open and proactive approach to managing risk that considers both threat and opportunity', where 'examples of good risk management practice are communicated by senior executives' and where 'individuals that excel in demonstrating good risk management practice in their day-to-day responsibilities are rewarded.' Different organisations have different risk appetites and strategies. Positive risk culture will not look the same in every entity, and will involve different things at each level of an entity. In particular, the management and governance arms of an organisation each have distinct and vital roles to foster effective risk culture.

