Risk management

Section Menu

Risk management

Successful risk management focuses on outcomes as opposed to being rules-based and process-driven. The embedding of a risk-awareness culture in an agency is also important to ensure it achieves its objectives.

Corruption risk management deals with risks that could facilitate corrupt conduct in an organisation. It has the potential to create opportunities to strengthen an organisation's core processes and functions. A key challenge, however, is ensuring that a corruption risk-management approach is based on a detailed understanding of the operational processes and contexts that may allow corruption to occur. If this does not occur, an agency may implement corruption controls that result in a suite of measures disconnected from the functioning of an organisation. These controls may be effective in controlling corruption, but they can also hinder efficiency and effectiveness. This leads to treatments that may not achieve the desired control at an acceptable cost to the agency.

NSW Government requirements for risk management

The NSW Treasury *Internal audit and risk management policy for the NSW public sector* (TPP 15-03, July 2015) mandates that all NSW public sector agencies have an organisation-wide risk management framework that covers the breadth of their activities. The NSW Government has approved the application of the Australian/New Zealand Standard ISO 31000:2009 Risk management ("the Standard") on risk management for the NSW public sector. Treasury has developed a *Risk Management Toolkit for NSW Public Sector Agencies* (2012), which acts as a guide to the Standard and includes templates, guidelines and a case study.

The Standard defines risk as the effect of uncertainty on objectives. The definition emphasises the role an organisation's risk management system has in the delivery of its strategic direction. The Standard and toolkit both emphasise the need to closely integrate risk management with underlying decision-making and operational practices. The Standard recommends that:

…risk management should be part of, and not separate from, an organisation's practices and processes … Risk management issues should be considered across all levels and activities so that you can develop an agency-wide view of risks that can impact on the achievement of your agency's objectives.

The toolkit emphasises that organisational objectives cover the full range of activities undertaken by an agency and include operational objectives such as the effective and efficient use of resources.
In terms of the risk of corruption and fraud, most NSW agencies are governed by the Treasury Fraud and Corruption Control Policy (TC 18-02, April 2018). This policy requires agencies to develop and maintain a fraud and corruption control framework, which, among other things includes “risk-based preventative and detective controls”.

Approaches to corruption risk controls

The Standard can be applied to the management of fraud and corruption risks in much the same way as any other category of risk. However, there are a some important differences that are worth pointing out, as follows.

First, corruption risks deserve specific attention due to their unique nature; although, this does not mean adopting a narrowly focused treatment strategy. While many risks evolve through error or disaster, corruption involves people motivated to purposefully avoid or work around prevention controls and strategies. This element of human behaviour means that there will always be a risk of corruption in an organisation, no matter how strong the risk management systems in place. For this reason, corruption controls should be audited from time-to-time to determine whether they are working as intended. Because this auditing is based on the possibility of corruption or deliberate non-compliance, the relevant fieldwork (for example, sample selection, testing methodology and verification of data) may require additional rigour and independence.

Secondly, because most corruption, by its very nature, is secretive, under reported and challenging to investigate, it is difficult for agencies to obtain reliable data about its true likelihood and consequences. For similar reasons, staff often misjudge risk because they – quite understandably – find it unnatural to think like a corrupt person. This often leads to disagreements about risk ratings and the appropriate risk treatments.

Thirdly, agencies should adopt a number of controls that are specifically aimed at addressing the risk of corruption. These include but are by no means limited to:

- having policies and procedures that address corruption prevention, conflicts of interest, gifts, and public interest disclosures
- training staff and contractors in ethics and the code of conduct
- having an investigative function
- segregating high risk functions.

Areas that are known to carry high risk, such as procurement, finance, recruitment and regulation, are also likely to have specific corruption controls. These controls are typically owned by staff with designated corruption-control responsibilities.

However, because corruption, waste and inefficiency are all correlated, the Commission strongly recommends that agencies also focus on controls that are aimed at optimising their business operations. For example, “What is the risk of not managing budgets tightly?”, is a more effective question than, “How do we stop the budget being skimmed?”. So if a frontline manager has a set of controls to efficiently manage their budget, many of the relevant corruption risks will be addressed at the same time. With this approach, agencies are in a good position to “design out” corruption risks as part of their day-to-day management of business risks, as opposed to bolting on corruption controls that may be resisted.

Fourthly, mapping key processes is a useful way to identify risk areas in an organisation. Mapping can be used to differentiate high-, moderate- and low-risk process steps and decision points, and to provide guidance in terms of which control might be most appropriate. In particular, process mapping is a good way to identify staff that have excessive or complete control over a particular function.

Fifth, the consequences of risks occurring together can be greater than if they occur in isolation. For example, the consequences of a *simultaneous* IT back-up failure and data corruption are greater than the consequences of each occurring in isolation. Risks can also trigger other risks; for example, unmanaged corruption risks can trigger safety risks. The consequences and interaction of risks should be taken into account.

Finally, during a high-level risk assessment, the easiest consequences to quantify are financial, and this can skew risk ratings, especially in agencies with large budgets. Yet, it may be the *reputational* costs of corruption that have the greatest impact on a public sector organisation rather than financial costs.

Updated November 2018