Chapter 2 – Risk management system

The topics covered in this chapter are:

- Taking a risk-based approach
- The legislative requirements
- The risk management process
- Recordkeeping
- Oversight of risk management
- Monitoring the process
- Best-practice targets

Taking a risk-based approach

Developing an effective fraud and corruption control program requires a comprehensive understanding of an organisation's risks and vulnerabilities. Identifying an organisation's key fraud and corruption risks is therefore one of the major tasks to be undertaken.

Risk assessment establishes an organisation's risk profile and the nature of the operating environment so that cost-effective practices can be established to contain or minimise each risk. The risk management process provides a logical development framework and methodology from which flow many of the elements of a fraud and corruption control plan — internal controls, reporting systems, the conduct of investigations, and training and awareness activities.

Risk management is good management practice. It is not an "optional extra", to be considered in isolation. It should permeate the organisation's activities and become a normal part of doing business.

The legislative requirements

Risk management is an important element of responsible administration, as set out in the *Financial Accountability Act 2009* (FA Act) and the *Financial and Performance Management Standard 2009* (FPMS).

This legislation requires department's accountable officers and statutory bodies to "adopt a proactive approach in monitoring the appropriateness of systems, operations and overall financial position and performance" of their organisation (FPMS, section 4), and to "establish a governance framework that includes a risk management system" (FPMS, sections 7 and 15).

A risk management system must provide for mitigating the risks to the department or statutory body and the State from unacceptable costs or losses associated with the operations of the department or statutory body, and managing the risks that may affect the ability of the department or statutory body to continue to provide government services. The accountable officer or statutory body may establish a risk management committee, in which case they must have regard to the "Audit committee guidelines – Improving Accountability and Performance", (Queensland Treasury) (FPMS, section 28).

Departmental heads of Internal Audit are responsible for providing advice and assistance with respect to risk management (FA Act, section 78).

The Local Government Regulation 2012 section 164 obligates local governments to keep a written record stating:

(a) the risks the local government's operations are exposed to, and

(b) the control measures adopted to manage the risks.

The risk management process

Risk management consists of the identification and analysis of risk, proceeds to threat assessment and evaluation, and goes through to the final selection of appropriate counter measures.

Australian Standard AS/NZS ISO 31000:2009 recommends a five-step risk management process:

(1) Establish the context

(2) Identify the risks

(3) Analyse the risks

(4) Evaluate the risks, and

(5) Treat the risks.

An alternative risk management methodology is provided in the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Fraud Risk Management Guide* (2016) and described in the *Fraud Risk Management Guide: Executive Summary* (2016).

Good communication and extensive consultation with internal and external stakeholders are very important at each stage of the risk management process. The success of the program depends on the extent to which everyone contributes to the assessment of risk and embraces the philosophy of actively managing it. (*AS/NZS ISO 31000:2009*, p.14).

1. Establish the context

> "If you lose money for the firm … I will be very understanding. If you lose reputation for the firm, I will be ruthless." Warren Buffett (to Salomon Brothers employees, 1991)

Different organisations face different fraud and corruption risks, and the first step in risk management is to establish the context of an organisation's risk exposure. *AS/NZS ISO 31000:2009* sets down a number of factors for consideration, which fall into four areas:

- **The external context.** What is the current relationship between the organisation and its environment and interested stakeholders? What are the crucial elements that may affect how the organisation manages the risks it faces?
- **The internal or organisational context.** What are the culture, current goals, objectives, strategies and capabilities of the organisation?
- **The task or activity context.** What are the objectives and strategies of the activity or function to which the risk management process is being applied?
- **The risk criteria.** What criteria are being used to evaluate the significance of the risks?

2. Identify the risks

Unidentified risks cannot be planned for and treated. However, the consequences of "risk types" can be anticipated and planned for. A full understanding of the organisation's exposure to risk will only come from a comprehensive search by all stakeholders for potential risks. The broader the range of stakeholders involved, the more likely it is that all risks will be identified.

The risk analysis must consider not only current threats from internal and external sources but also potential and emerging threats.

Using a variety of techniques helps to identify risks. The search for potential risks may include reviewing the organisation's fraud register and records of prior losses for ongoing risks and trends; analysing process flow charts; interviewing clients and conducting group discussions; analysing audit outcomes; conducting SWOT (Strengths, Weaknesses, Opportunities and Threats) and gap analyses; control risk assessments; scenario analyses; and brainstorming. An inquiring mind is invaluable in identifying potential risks.

Potential risks should not be overlooked or filtered out by premature judgments. The important thing is to adopt a systematic and comprehensive approach so that all potential risks are identified, regardless of their source or controllability.

An organisation may face major challenges in identifying its fraud and corruption risks. In some cases, an organisation's context and the industry environment may highlight particular functions or make some classifications of risk more significant than others.

One starting point is to identify the organisation's major activities, and the nature of the business activities carried out by internal groups on external activities, and the degree to which these internal groups interact with the external entities, such as:

- service outputs and deliverables
- operational areas and functions
- revenue generation and collection activities
- expenditure programs and financial management
- outsourced or contracted operations
- supplier interfaces and other service inputs
- asset utilisation, acquisition and disposal
- client records and support.

Another approach is to build on the work of others and seek out similar bodies that may be willing to share experiences. Consulting firms also often have industry-based and sector-based checklists that can be useful.

Areas of risk to explore

The CMC survey *Profiling the Queensland public sector* (CMC 2004) provides an insight into operational areas and functions perceived to have high levels of fraud and corruption risk, including:

- financial functions – such as the receipt of cash, revenue collection and payment systems, salaries and allowances, entertainment expenses
- construction, development and planning functions – ranging from land rezoning or development applications to construction and building activities
- regulatory functions – involving the inspection, regulation or monitoring of facilities; and operational practices, including the issue of fines or other sanctions
- licensing functions – such as the issue of qualifications or licences to indicate proficiency or enable the performance of certain activities
- demand-driven or allocation-based functions – where demand often exceeds supply, including the allocation of services or grants of public funds, or the provision of subsidies, financial assistance, concessions or other relief
- procurement and purchasing functions – including e-commerce activities, tendering, contract management and administration, and the practices of external agents/contractors/consultants and providers of goods/services
- other functions involving the exercise of discretion, or where there are regular dealings between public sector and private sector personnel (especially operations that are remotely based or have minimal supervision).

3. Analyse the risks

Once the risks have been identified they need to be analysed and assessed to determine their significance so they can be prioritised for treatment.

There is no single template or model for risk assessment. AS 8001:2008 suggests a separate approach for every exercise, but that may not be feasible. The essential requirement is that the method used meets the needs of the organisation — and every organisation is unique.

The most common form of risk analysis is through application of sound judgement or informed decision-making, often known as "qualitative risk analysis". This is done by assessing how likely it is that an event will happen or how frequently it might occur, and determining how serious the potential consequences would be if the event occurred. This process should be undertaken by people within the organisation with sufficient practical experience and a depth of understanding about the organisation and the risks associated with business operations.

Figures 2.1, 2.2 and 2.3 are sample tables for this purpose. Note that each organisation should develop label descriptions to suit its own processes and operating environment.

Figure 2.1: Likelihood scale

Rating	LIKELIHOOD – What is the likelihood of the risk event occurring?
5	**ALMOST CERTAIN:** will probably occur, could occur several times per month
4	**LIKELY:** high probability, likely to arise once per month
3	**POSSIBLE:** reasonable likelihood that it may occur at least once in a year
2	**UNLIKELY:** plausible, could occur over a five-year period
1	**RARE:** very unlikely but not impossible, unlikely over a five-year period

Figure 2.2: Loss or damage impact scale

Rating	IMPACT – What is the potential loss / damage / impact if the event occurs?
5	**EXTREME**: Loss of life, or significant injury. Loss of millions of dollars, major reputational damage
4	**MAJOR**: Organisation's major objectives threatened, or severely affected
3	**MODERATE:** Has some impact on achieving objectives, and requires considerable effort to rectify
2	**MINOR:** Impact on objectives; with some effort, objectives can still be achieved
1	**INSIGNIFICANT:** Very small impact, rectified by normal processes

Combining the assessment of likelihood with the assessment of impact produces a qualitative risk analysis of the seriousness of the risk (Figure 2.3).

This provides a comparative measure for each risk to assist in the evaluation process to guide decision making about the priority of treatment or urgency of action.

Figure 2.3: Qualitative risk analysis matrix

LIKELIHOOD	IMPACT				
	Insignificant	**Minor**	**Moderate**	**Major**	**Extreme**
Almost certain	Medium	Medium	**High**	**Severe**	**Severe**
Likely	Medium	Medium	Medium	**High**	**Severe**
Possible	Low	Medium	Medium	Medium	**High**
Unlikely	Very low	Low	Medium	Medium	Medium
Rare	Very low	Very low	Low	Medium	Medium

4. Evaluate the risks

Risk evaluation involves comparing the level of risk found during the analysis process against the risk criteria established when the context was considered (*AS/NZS ISO 31000:2009*. p. 18).

The evaluation needs to take into account all the factors relevant to the organisation. This is likely to include the impact on the organisation's ability to meet its strategic objectives and continue its operational functions, monetary considerations, the organisation's reputation and employee morale.

The risk evaluation process will help organisations decide on the course of action to take, including:

- whether an activity should be undertaken
- whether a risk needs treatment
- priorities for treatment.

The decisions made should be recorded – a simple risk evaluation worksheet will help with this (Figure 2.4).

Figure 2.4: Risk evaluation worksheet

IDENTIFICATION		ANALYSIS			EVALUATION	TREATMENTS
Area being assessed	**Specific risks**	**Risk degree**			**Current controls or mitigating factors**	**Control improvements**
		Likelihood	**Consequences**	**Risk rating**		

Likelihood	**Consequences**	**Risk rating**
A = Almost certain	1 = Insignificant	S = Severe risk — immediate action required
B = Likely	2 = Minor	H = High risk — senior management attention required
C = Possible	3I = Moderate	M = Medium risk — management responsibility must be specified
D = Unlikely	4 = Major	L = Low risk — manage by routine procedures
E = Rare	5 = Extreme	VL = Very low risk – monitor only

Applying the risk analysis process consistently will identify the risks that need further treatment, and will result in a prioritised list of risks that require consideration in the current period.

5. Treat the risks

The next step is to determine the measures available for treating the risks, assess the treatment options, and prepare, prioritise and implement suitable risk treatment plans (*AS/NZS ISO 31000:2009*, pp. 19–20). Risks are commonly treated using one or more measures that involve:

(1) Accepting the risk

(2) Reducing the likelihood of the risk occurring

(3) Reducing the consequences if the risk occurs

(4) Transferring the risk in full or in part to another party, often contractually or through insurance

(5) Avoiding the risk by deciding not to start or not to continue an activity.

The treatment to be applied to each risk depends on the risk appetite of the organisation and the feasibility and cost-benefit analysis of the available control measures. Every available option should be explored, rather than just adopting the first or most obvious answer.

Risks that fall into the very low, low or acceptable categories may be accepted without further treatment. These risks should be monitored and periodically reviewed to ensure they remain acceptable. Risks in all other categories are to be treated.

Integrity risks require special consideration. It is broadly accepted that a person with integrity will always do the right thing and follow the rules, even when no-one is watching. The challenge for organisations seeking to create a culture of integrity is to set conditions such that people willingly meet those expectations. However, a realistic appraisal of an organisation's integrity risks will include the likelihood that not everyone will consistently act that way. To cater for this, organisations need to set ethical boundaries by means of their policies and procedures. Ultimately, individuals are responsible for exercising their personal integrity through balancing personal interests against the requirements of the organisation and ensuring they make decisions in the public interest. Consequently, organisations should focus on reducing the occurrence of personal integrity failures by reducing the likelihood they will occur. This is achieved by communicating the boundaries and the consequences of failing to adhere to them through regular training, rather than by simply accepting the risk.

The outcome will be a prioritised risk treatment plan that documents the chosen options and how they will be implemented. The plan should include:

- proposed actions
- resource requirements
- responsibilities
- timing
- performance measures
- reporting and monitoring requirements. (*AS/NZS ISO 31000:2009*, p. 20).

Recordkeeping

The process

Every stage of the risk management process involves a wealth of information that can provide:

- a history that allows users to look at previous treatments and how they were implemented to see what worked and what didn't, and so provides an insight into better options
- legal protection – claims of negligence may be defeated or minimised if it can be shown that attempts were made to identify and treat risks
- the means for satisfying external reviews such as independent audits.

To enable this, there should be good quality documentation that includes:

- the results of the appraisal or risk assessment
- the action required as a result of the appraisal or risk assessment
- the reasons and rationale as to why particular treatments were chosen for implementation, including considerations such as cost, ease of implementation and likely effectiveness
- recommendations for follow-up action.

This ensures that the methodology can be replicated to deal with future developments or changes.

Decisions

All decisions made during the risk assessment process should be recorded in a **fraud risk register**, together with the reasons for the decisions (*AS/NZS ISO 31000:2009*, p. 20).

The information below provides guidance regarding the structure of a fraud risk register.

Fraud risk description	The fraud risk is described, ensuring that both the cause and impact of the risk eventuating is covered in the description provided.
Fraud risk factors	These are the conditions or actions which are most likely to cause the risk to eventuate. This is generally a brief list of likely scenarios that could occur.
Inherent likelihood	This provides an indication of how often the risk might eventuate in the absence of any controls. This is generally measured using a five-point scale, e.g. almost certain, likely, possible, unlikely, rare.
Inherent consequence	This provides an indication of how serious the consequences would be if the risk eventuated in the absence of any controls. This is generally measured using a five-point scale, e.g. extreme, major, moderate, minor, insignificant.
Inherent risk rating	This provides a ranking for the risk once the likelihood and consequence of the risk has been considered in the absence of any controls. This is generally measured using a five-point scale, e.g. severe, high, medium, low, very low.
Key controls identified	The key controls are those controls currently established in the entity to minimise the likelihood and consequence of the risk eventuating.
Residual likelihood	This provides an indication of how often the risk might eventuate taking into consideration the effectiveness or otherwise of existing controls. This is generally measured using a five-point scale, e.g. almost certain, likely, possible, unlikely, rare.
Residual consequence	This provides an indication of how serious the consequences would be if the risk eventuated taking into consideration the effectiveness or otherwise of the existing controls. This is generally measured using a five-point scale, e.g. insignificant, minor, moderate, major, extreme.
Residual risk rating	This provides a ranking for the risk once the likelihood and consequence of the risk has been considered taking into consideration the effectiveness or otherwise of the existing controls. This is generally measured using a five-point scale, e.g. severe, high, medium, low, very low.
Fraud risk owner	This is the individual or group within the entity with accountability for managing the identified fraud risk.
Action required	This includes any further actions that the entity must undertake in relation to the identified fraud risk (i.e. new controls to be established).

The Fraud Risk Register is best kept as a separate document from other risk registers as it may also contain sensitive information which not should be more widely accessible than is necessary. This also facilitates monitoring.

Oversight of risk management

Appropriate resourcing and stewardship is needed to make fraud and corruption risk management effective. Clearly designated responsibility for the organisation's fraud and corruption control initiatives will greatly assist communication with all stakeholders, particularly where there is a reporting obligation external to the organisation. It will facilitate developing, implementing, maintaining and reviewing every aspect of the program.

Even if all or part of the risk assessment and policy development tasks are outsourced, overall responsibility for implementing the program should be assigned to a senior officer as part of their normal duties. That person should be a member of any general risk management committee that the organisation sets up. The responsible officer can play an important role in ensuring that the methodology is appropriate, and can help to improve corporate understanding and commitment to the process.

A risk management committee can also be a good source of advice for building an integrated approach to fraud and corruption risk management. The committee can be responsible for:

- overseeing the development of integrated and cost-effective risk management plans
- monitoring the effectiveness of risk management programs
- reporting to senior management on risk-related issues
- integrating fraud and corruption matters with the organisation's overall risk profile
- disseminating information on risk issues throughout the organisation.

Regardless of whether the oversight function is carried out by an individual or a committee, it is critical that the product of this work is captured in the organisation's policies and procedures, which are to be reviewed and updated to address emerging risks.

Given the diversity of risk and its impact on different stakeholders, strong communication programs are needed to guarantee good levels of understanding and consistent operational practices. Education, awareness and communication are discussed in Chapters 9 and 10.

Monitoring the process

Organisational systems and operating environments are constantly changing, and few risks remain static. Consequently, risk identification and assessment (including treatment plans, strategies and control mechanisms) need to be part of a continual review process rather than a one-off event (*AS/NZS ISO 31000:2009*, p. 20).

In addition to continually monitoring the effectiveness of the risk management process, specific events may happen which would trigger a review. Examples of triggers include:

- a fraud or attempted fraud – these will reveal vulnerabilities that had been previously overlooked, or reveal a need for additional controls
- changes in the operating environment – removal of old or implementation of new operating systems and practices can create and/or eliminate risks for an organisation
- identification of emerging risks.

The *Australian Standard AS 8001:2009* recommends a comprehensive review of fraud and corruption risks every two years, depending on circumstances (p. 20). These reviews should consider the organisation's risk exposure in the current environment, threats from both internal and external sources, and emerging risks. The effectiveness of the controls should also be reviewed at this time. This continual process of monitoring and review will ensure that the risk criteria are critically examined and the control mechanisms improved in each review cycle.

Best-practice targets

(1) The organisation should assess fraud and corruption risks using a comprehensive risk management system to establish the level and nature of its exposure to internal and external threats (at least every two years).

(2) The assessment should cover all discrete functions and operations of the organisation.

(3) To ensure an integrated and consistent approach, the fraud and corruption risk assessment should form part of the organisation's overall risk management strategies.

(4) The process of risk evaluation should be based on a comprehensive understanding of the organisation's risk profile within the context of its particular operating environment.

(5) The organisation should allocate sufficient resources to carry out the risk identification and assessment tasks to capture all likely risks and treatment plans to mitigate risks.

(6) The organisation should consider taking out insurance to cover itself against fraudulent losses commensurate with its risk profile, and should review this policy annually.

(7) When dealing with integrity risk, wherever possible, focus on reducing the likelihood by providing adequate training rather than accepting the risk.

(8) The fraud risks and planned actions should be listed and prioritised in a Fraud Risk Register.

(9) The organisation should incorporate the outcomes of risk reviews and control responses into the overall corporate risk strategy to ensure that risk is managed in an integrated manner.

(10) A specific person or group should be made responsible, to ensure effective leadership, coordination and accountability for this process.

Additional readings

- *Australian Standard AS/NZS ISO 31000:2009 – Risk Management – Principles and Guidelines*
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2016 – *Fraud Risk Management Guide*
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2016 – *Fraud Risk Management Guide: Executive Summary*
- Department of Finance, Risk Resources. <www.finance.gov.au/comcover/policy/risk-resources.html>

Checklist: Risk management system

The following questions are indicative only. Each organisation should develop its own checklist to reflect its specific needs and risk environment. The checklist should be re-examined and updated periodically, as part of the organisation's program of fraud and corruption control appraisal.

Legislative requirements

- ☐ Does the organisation have a risk management system? (FAA section 61 (b), FPMS sections 7 and 15(1)(h))
  If yes,
  - ☐ Is it reviewed regularly (at least every two years) to ensure it is still appropriate? (FPMS section 15 (3))
- ☐ If there is a risk management committee, does it have regard to the "Audit committee guidelines – Improving Accountability and Performance", (Queensland Treasury) (FPMS, section 28)?

Recommended Best Practice

- ☐ Does the organisation's risk management system cover fraud and corruption risks?
- ☐ Does the organisation have a comprehensive program of fraud and corruption risk assessment?
- ☐ Does the program of risk assessment use a methodology consistent with the *Australian Standards AS8001: 2008: Fraud and Corruption Control Guidelines* 3.6 and *AS/NZS ISO 31000:2009: Risk Management*?
- ☐ Is the organisation's risk review and assessment process thoroughly documented?
- ☐ If a fraud and corruption risk assessment has been conducted, did it:
  - ☐ actively involve all relevant stakeholders
  - ☐ capture all of the organisation's at-risk functions
  - ☐ establish the vulnerability of business processes and related tasks or activities
  - ☐ identify likely internal and external threats
  - ☐ take account of both current and possible future threats
  - ☐ review data from the organisation's fraud register
  - ☐ rate the probable risks appropriately
  - ☐ consider appropriate controls to both prevent and detect fraud
  - ☐ prioritise the implementation of control treatments accordingly
  - ☐ result in a prioritised treatment plan that documents the chosen options and how they will be implemented
  - ☐ ensure adequate communication
  - ☐ properly store the results to enable accessing this information in the future?
- ☐ Does the organisation have a separate fraud risk register?
  If yes:
  - ☐ Is the Fraud Risk Register reviewed regularly by Internal Audit?
- ☐ Is there a person nominated (or designated committee or taskforce) to be responsible for overseeing the assessment of fraud and corruption risks and any relevant control program?
- ☐ Is there a representative and knowledgeable advisory committee to oversee risk management and provide advice and support to any nominated officer, group, committee or taskforce?
- ☐ Has a comprehensive risk assessment been carried out or has the previous assessment been comprehensively reviewed less than two years ago?

- ☐ If there are indications that reviews of risk exposure in particular areas should be carried out more frequently than every two years, has this been done?
- ☐ If there have been any major changes to the organisation's structure, functions or operating environment in the last two years has a risk review been completed since?
- ☐ Are there mechanisms to generate a risk review in the event of legislation changes?
- ☐ Is there a system for recording and monitoring fraud and corruption incidents?
- ☐ Is there a process to trigger a review in response to a fraud event?
- ☐ Are the fraud or corruption incident records maintained in a fraud or corruption register?
- ☐ Are fraud or corruption incidents analysed (for the purpose of identifying trends and emerging threats) at the time that other organisation risk assessments are carried out?