Chapter 3 – Internal controls

The topics covered in this chapter are:

- The significance of internal controls
- The legislative requirements
- The essentials of internal control
- Responsibility for internal controls
- The limitations of control
- Monitoring effectiveness
- Reporting on controls
- Best-practice targets

The significance of internal controls

Internal controls are considered by many to be the first line of defence in the fight against fraud (*AS 8001:2008*, p.29).

Once an organisation has established its risk profile through a comprehensive risk assessment process, it can establish internal controls to deal with and minimise those risks.

> Internal controls cannot guarantee that there is no error or fraud. They can, however, reduce the risk of error and fraud occurring in the first place, and can help to detect fraud and error where it has occurred. (QAO Report 5, 2012, p. 5)

The legislative requirements

State government

For Queensland government departments and statutory bodies (as defined in the *Financial Accountability Act 2009*), internal controls are mandated in two key pieces of legislation, both of which relate to financial management and accountability:

- *Financial Accountability Act 2009* (FA Act)
- *Finance and Performance Management Standard 2009* (FPMS).

The legislation deals with public sector financial management through a principles-based approach, requiring accountabilities and outcomes, rather than prescribing processes. This is a substance-over-form approach, which provides organisations with the flexibility to manage their operations in the most cost effective manner. It allows organisations to develop and implement systems of internal control which best suit their circumstances while still meeting prescribed accountability requirements.

The requirement to establish an internal control structure is found in the FA Act section 61 and the FPMS section 8.

The prescribed accountabilities in the FPMS section 8 are as follows:

- The internal control structure must have a strong emphasis on accountability, best-practice management of the resources of the organisation and internal controls, and must include:
  - an organisational structure and delegations that are supportive of the objectives and operations of the organisation
  - employment of qualified and competent officers, training of the officers and assessment of their performance
  - procedures for monitoring the performance of, and accounting for its investment in, any other entity controlled by the organisation
  - mechanisms to ensure the efficient, effective and economic operation of any internal audit function, audit committee or risk management committee.
- In establishing the internal control structure, the accountable officer or statutory body (section 65 FA Act) must have regard to the *Financial Accountability Handbook* published by Queensland Treasury.
- The internal control structure must be clearly set out and explained in the financial management practice manual of the organisation.
- To the extent practicable, an accountable officer or statutory body must ensure there is an appropriate separation of duties between officers of their organisation.

In addition, section 29 of the FA Act creates a requirement for accountable officers to establish an internal audit function. Statutory bodies are to establish an internal audit function if their Minister so directs or if the statutory body considers it is appropriate to do so.

Section 15 requires accountable officers and statutory bodies to regularly review key governance and control systems to ensure they remain appropriate for managing the financial resources of the department or statutory body.

Under the FA Act:

- Public Service departments' CFOs are also responsible for the establishment, maintenance and review of financial internal controls, and then reporting on the internal controls in an annual statement to the accountable officer (section 77). (Also the FPMS section 57.)
- Departmental heads of Internal Audit are responsible for providing advice and assistance with respect to internal controls and risk management (section 78).

Local government

For Queensland local government, the key piece of legislation that mandates internal controls is the Local Government Regulation 2012 (LG Reg).

LG Reg section 164 states that a local government must keep a written record stating:

- the risks the local government's operations are exposed to, to the extent they are relevant to financial management, and
- the control measures adopted to manage the risks.

The essentials of internal control

Effective internal control requires an integrated internal control structure. This structure consists of the policies, procedures, processes, tasks and other tangible and intangible factors put in place by an organisation to manage operational, financial, compliance or any other type of risk. An effective system should safeguard the organisation's assets, facilitate internal and external reporting, and help the organisation comply with relevant legislation.

An internal control structure is comprised of:

- the control environment
- the internal controls themselves
- processes for monitoring effectiveness.

The control environment

An effective control environment is fostered by clearly stated policies and procedures and well-defined responsibilities and accountabilities that ensure the appropriate use of the organisation's assets.

A number of components are required, including the following:

- **Leadership** – Senior management provides a powerful role model in setting the ethical tone of the work environment and in maintaining an appropriate internal control culture. This is achieved through a participative and transparent management style that models, promotes and supports the desired culture. This includes setting and monitoring realistic goals, objectives and expectations. Managers should aim to demonstrate through their leadership, words and actions that they enforce and monitor the organisation's controls, and are themselves subject to those control constraints.
- **Organisational culture** – A culture that recognises the importance of supervisory accountability will reduce the incidence of fraud and corruption. (See Chapter 9).
- **Organisational structure** and **reporting structure** – A clear organisational and reporting structure ensures that every employee understands what they are responsible for and to whom they are accountable. This clarity also ensures that supervisors and managers understand their reciprocal obligations to monitor the activities, processes and outputs of their subordinates to ensure timely, accurate and quality work is produced in accordance with the control environment.
- **Delegations and approval processes** – The organisation needs to have clearly documented delegations and approval processes that are monitored. These place an emphasis on accountability, consistent with the focus of the FA Act.
- **Audit and risk oversight** (see Chapter 1 for more information.)
  - Internal audit is a valuable function which significantly strengthens the control environment. Departments are required under the FPMS (section 29(1)) to have an internal audit function. Statutory bodies are required to have one if so directed by the relevant Minister or by their board (FPMS section 29(2)). The internal audit function can be in-house or outsourced. In either case the organisation is still deemed to have an internal audit function. Any internal audit function must have a charter that is consistent with the auditing and ethical standards set by the relevant professional bodies (FPMS section 30).
  - An accountable officer must, and a statutory body may, establish an audit committee for their organisation, having regard for the guidelines, *Audit Committee Guidelines – Improving Accountability and Performance (2012)*, prepared by Queensland Treasury (FPMS section 35). An audit committee is designed to discuss issues identified by the internal and external audit functions and to provide independent advice to the accountable officer or statutory body.
  - The relationship between internal and external audit is also significant – it is important to recognise the limitations of the external audit function and the way it links with internal audit and compliance activities.
- **Employment of qualified and competent officers** – This requires adequate employment screening**.** A number of checks should be conducted before employing staff. These include: referee checks, verifying stated qualifications (particularly when qualifications are a requirement for a position), criminal history checks and disciplinary history checks. In addition, periodic checks of existing employees in high risk areas should be considered.

Department chief executives are required by Public Service Directive 07/11 – *Employment Screening*, to: (i) conduct employment screening for persons engaged, or proposed to be engaged, to perform relevant duties or prescribed duties in the Queensland public service, and (ii) implement a risk management strategy for agencies performing child-related duties.

The *Public Service Act 2008* (PS Act) Chapter 5, Part 6 (sections 150 to 186) provides for criminal history checks to be obtained and used as a means of determining employment suitability. These sections apply across a range of circumstances including regulated employment and child-related duties.

There are legislated screening requirements under the *Working with Children (Risk Management and Screening) Act 2000* for child-related employment, businesses and service providers. There are also specific requirements for the provision of services and care for people subject to the *Child Protection Act 1999*, the *Public Guardian Act 2014* and the *Family and Child Commission Act 2014*.

Organisations are obligated to conduct a full appraisal about the provision of services, the range of locations and circumstances in which these services may be provided, and implement appropriate responses where interaction with clients subject to the Acts discussed above can reasonably be anticipiated.

Where appropriate, a chief executive must also comply with screening requirements under Commonwealth and State legislation (e.g. security clearances and other background checking) which are not covered by the PS Act Part 6.

- **Code of Conduct** – This is a key document for describing the standards of conduct that are expected of public officers to ensure that their conduct is consistent with public sector ethics principles and values. The provisions of a code of conduct support many of the operational practices designed to minimise fraud and corruption risks. Public service agencies and public sector entities' codes are underpinned by the PSE Act, which makes contraventions of an organisation's code grounds for disciplinary action (PSE Act section 4). (See Chapter 8 for more information.)
- **Human Resources policies and practices** – These should anticipate the information needs of all employees and be written in plain English to provide clear, unambiguous guidance and standards. Information about the possible consequences of failing to adhere to the organisation's code of conduct, policies and practices should be made clear to staff.
  - The PSE Act section 24 gives directions regarding the basis for disciplinary action for contraventions of an organisation's code of conduct.
  - For the public service the grounds for discipline and the appropriate available disciplinary actions are specified in the PS Act, primarily in sections 186 to 192. The *PSC Guideline 01/17: Discipline* provides additional guidance on this.
  - For local government councillors, the LG Act applies.
  - Other organisations should develop separate written disciplinary policies and processes and give consideration to addressing conduct matters in performance agreement schemes.

Internal controls

Internal controls need to cover more than just an organisation's financial operations. They must cater for other aspects of operational performance, compliance and "corporate health".

Internal control systems should be designed to suit the individual organisation. Although many internal control practices have a common application, such as the separation of functions and a well-developed system of accountability, there is no "one-size-fits-all" set of internal controls that can simply be applied across all organisations.

To formulate controls for your organisation, begin with the identified set of fraud and corruption risks and proceed to an assessment of the possible internal control measures matching those risks. The use of control checklists may be helpful, but nothing substitutes for a detailed risk assessment and

treatment process tailored to the organisation and its operating environment. (See Chapter 2 for more information.)

Internal controls can take many forms. They can be simple procedures such as locking doors or limiting access, or processes that are built electronically into a system. They can also extend to more direct and intrusive supervision such as video surveillance of activities. Some of the most effective controls can be quite straightforward. For example, simply ensuring transparency of operations can have a powerful control impact, both internally and with external stakeholders. This could include placing details of tender processes and approved tenders on the organisation's website. The organisation's financial management practice manual is a control (FPMS section 16(3)(c)). More sophisticated controls may include data mining techniques that analyse expenditure patterns and uncover discrepancies in claims and payments.

Avoid having too many controls, or controls that are unduly restrictive. This can lower productivity and increase bureaucracy, thereby inviting noncompliance and shortcuts that increase risk. It is also pertinent to periodically test your controls to ensure they are working.

The *Australian Standard AS8001:2009* (p. 29) notes that the organisation's internal controls should be:

- appropriately documented
- subject to continuous improvement
- risk-focused
- effectively communicated to all stakeholders
- accessible to all personnel.

Processes must be documented and the documents must be readily available to all employees.
The organisation must provide employees with adequate and ongoing training in the processes.
The processes must be followed by the department or statutory body.

The following is a summary of some common types of internal controls.

Separation of duties – This is a well-known control principle that can be applied to nearly all business processes and systems, and is required under the FPMS (section 8) wherever practicable. It works by ensuring that no one person has complete control over all aspects of a transaction, record or resource. The separation of duties principle can be applied in various ways to many activities. It may involve physical access controls, the division of duties, or giving different security access levels for information.

Contractor screening – Using external providers of goods and services can be a high risk activity, and requires suitable controls such as pre-approval screening to reduce the risks. Consider pre-contract due diligence, reference and finance checks.

Contract management – For some high-risk externally provided goods or services, consider including contractual obligations that require the supplier and their staff to comply with your key integrity policies, such as the code of conduct, information security and gifts and benefits. Importantly, ensure that conflicts of interest provisions are included. If contracts are already established, review how the initial contacts with the provider were made and check for any possible conflicts of interest. Also conduct a risk assessment to identify other relevant controls.

For contractors in lower risk categories, giving them adequate information regarding the agency's policies and procedures and its code of conduct can also help by ensuring they know what is expected of them in their dealings with the organisation's staff. (See Chapter 10 for more information.)

All contractors should be advised that failure to adhere to these requirements will result in the contract being reviewed, which may well result in it being terminated. Additionally, if the contractor's conduct raises the suspicion that criminal action has occurred the matter will be reported to the appropriate authority (i.e. the QPS, and the CCC).

Information security systems – An organisation's information is a valuable asset that must be protected by a comprehensive fraud and corruption control program. This includes raw data and transaction records. Consequently, secure management of information resources lies at the heart of most organisations' operations. The increasing incidence of computer hacking makes this even more critical.

Management information and accounting systems are critical components of an organisation's internal control systems. Organisations must have control processes to ensure that the use of information is always legitimate, relevant and impartial in serving the public interest. Consideration must also be given to how that information is securely stored and processed, and how it is used in the organisation's decisions.

The Queensland Government *Information Standard 18: Information Security* (IS18) requires that organisations develop, document, implement, maintain and review appropriate security controls to protect the information they hold by:

- establishing appropriate information security policy, planning and governance within the organisation in line with this information standard, including adopting all specified frameworks, standards and reporting requirements
- ensuring appropriate security controls are implemented as detailed by this information standard and its supporting documents.

Internal controls are also essential to reduce the risk of inaccurate public records being created or public records being disposed of improperly. *Information Standard 40: Recordkeeping* (IS40) and *Information Standard 31: Retention and disposal of public records* (IS31) contain information on developing and implementing recordkeeping controls and protocols. Queensland State Archives can provide further guidance on strategies for developing and implementing these controls. The CCC Advisory, *Management of public records* provides information about the corruption risks associated with poor records management and strategies to prevent corruption.

Key controls include:

- an auditable log which records all instances of access to critical or sensitive information, and regular review of this log.
- processes to ensure that users' levels of access and combinations of access are appropriate for their role
- user-maintenance procedures, such as locking and deleting accounts when a person resigns
- controls over passwords, including requiring sufficiently complex passwords, regular password changes, and adequate checks before password changes are permitted
- adequate management of software patches (a poorly designed and implemented software patch, designed to fix problems, can sometimes introduce new problems)
- adequate integration or reconciliation where more than one system is in use
- regular tests to ensure your gateways, firewalls and security systems will resist hacking or disruption.

Controls for small organisations

In small organisations the practical arrangements for internal controls may differ. Hands-on management can provide good control and compensate for the absence of more formal control arrangements. For example, in some small organisations, even the board may need to take on additional oversight roles, such as approving cheque runs, or payment schedules.

Managers will often be able to identify incorrect data and significant variances from what they expect, and their direct knowledge of client concerns and informal communication can quickly draw attention to operating or compliance problems.

Small organisations may find it difficult to achieve an appropriate separation of duties. Whenever possible, duties should be assigned so as to provide suitable checks and balances. If this is not possible, management may need to supervise operations more directly. For example, expenditure authorisation might be restricted to the manager.

A manager needs to "reach down" further into the operational activities of a smaller organisation and carefully review supporting documentation, bank reconciliations, invoices, orders, bank statements and other matters. The way information is received and handled may need review; for example, certain external statements and confidential internal reports may need to be delivered in unopened envelopes to a manager.

The need for management to be more hands-on may also increase the risk of management overriding key controls. Accordingly, there also needs to be appropriate oversight from those charged with governance, i.e. the accountable officer, audit committee or board.

Other resources

More information on internal controls can be found in Queensland Treasury's publication, *Financial Management Tools*, 2012.

Another useful resource is the Committee of Sponsoring Organizations for the Treadway Commission (COSO) that sponsored a body of work that has resulted in many standard internal control terms. One of the most significant COSO developments was the issue in 2004 of the updated definitive study, *Internal control: integrated framework*. This work was revised and reissued in 2016 as the *Fraud Risk Management Guide.*

Responsibility for internal controls

The CEO carries ultimate responsibility for an organisation's system of internal controls, but still relies on the support of management in fulfilling this role through well-structured lines of accountability. Creating a suitable control climate is facilitated by clear lines of accountability and appropriate organisational structures, suitable value statements, unambiguous position descriptions and service protocols, and effective operating policies and procedures.

Everyone in the organisation has a role to play in making sure that internal controls are working properly.

Managers are primarily responsible for implementing the controls and monitoring their effectiveness.

Line managers and supervisors are often in the best position to identify system deficiencies that facilitate fraud and corruption. Their job descriptions should reflect this responsibility, including an ongoing obligation to ensure that staff know and comply with the internal controls relevant to their roles.

Every employee should contribute to the development of better systems and procedures that will improve the organisation's resistance to fraud and corruption. To realise this objective, they need to know about the risks faced by the organisation and be encouraged to develop and adopt effective controls. In addition to following and complying with the control systems, they should report every detected failure of those systems to their managers.

The Australian Auditing Standard ASA 240 – *The Auditor's Responsibilities Relating to Fraud in an Audit of a Financial Report* states:

> The primary responsibility for the prevention and detection of fraud rests with both those charged with governance of the entity and management. It is important that management, with the oversight of those charged with governance, place a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals not to commit fraud because of the likelihood of detection and punishment. This involves a commitment to creating a culture of honesty and ethical behaviour which can be reinforced by an active oversight by those charged with governance. Oversight by those charged with governance includes considering the potential for override of controls or other inappropriate influence over the financial reporting process, such as efforts by management to manage earnings in order to influence the perceptions of analysts as to the entity's performance and profitability.

Accountability includes ensuring the operations of your controls, the expected standards of ethical and professional conduct, and the transparency of your decision making exceed the minimum standards set down by legislation and that the "spirit" underpinning these standards is willingly adopted rather than taken on as imposed.

The limitations of controls

Any control system is subject to limitations. There is always the risk that:

- a person will identify and take advantage of a control weakness
- two or more people may collude to circumvent the controls
- circumstances may cause a particular control to be omitted on cost–benefit grounds (a conscious risk treatment decision)
- errors of judgment may still occur, though effective controls will help detect and minimise any such occurrences
- a control will become ineffective over time due to changes in software, technology or organisational restructures, and that this will not be noticed.

It is not sufficient merely to have the controls in place. They must be exercised conscientiously and continuously, and not be allowed to fall into decay or disuse because employees are busy, overloaded or merely lazy. Every manager and supervisor has a primary responsibility to ensure that procedures and controls are followed faithfully.

An internal control system is not a guarantee of success, but it provides a cost-effective way of minimising fraud and corruption risks.

Monitoring effectiveness

The accountable officer or statutory body must ensure regular reviews of the systems used to manage the organisation's financial resources (FPMS section 15(3)). Continual monitoring and review of the organisation's internal control mechanisms should be part of the normal management process. Monitoring activities should feed into an annual reporting and audit program that assesses the controls and their effectiveness under any changed conditions or in the face of reported weaknesses.

Chief Finance Officers of departments are required under the FA Act section 77(2) and the FPMS section 57 to provide their Director-General with an annual statement on the effectiveness of internal controls. This type of reporting is highly recommended for all organisations.

The Queensland Audit Office states in its *Fraud Risk Management*, Report 9, 2013 that significant benefits can be gained by management running regular data analytics in a structured manner. Data analytics can quickly and efficiently uncover suspicious or anomalous patterns in transactions and can

examine large and complex data sets quickly, efficiently and consistently. Use of data analytics may, in itself, provide a deterrent to potential fraudsters.

The organisation's internal audit program should regularly review internal controls as well as auditing other more general procedural and compliance matters. To ensure an objective review that is beyond reproach, the organisation's audit program should be independent of any direct role in implementing internal controls or the fraud and corruption control program. These latter functions always remain a shared responsibility of line management.

If the organisation does not have an internal audit function, the need for one should be regularly reviewed. This can be done as part of the organisation's process for assessing the effectiveness of internal controls and evaluating internal compliance activities.

Reporting on controls

Each organisation should provide an annual statement of its risk management and control status, to reassure the public that all significant risk factors have been taken into account and that appropriate controls are operating. The level of disclosure needs to be comprehensive enough to give an accurate description of the organisation's operating environment. (See Chapter 10.)

The FPMS (section 49) directs that the requirements in the document, *Annual Report Requirements for Queensland Government Agencies* (prepared by the Department of the Premier and Cabinet) are adhered to. These requirements may change from year to year, but usually require agencies to disclose information about risk management, including providing reasons why an agency does not have an internal audit function.

Best-practice target

(1) The organisation should have a range of internal controls, designed to both prevent and detect fraud appropriate to its own operating environment and its specific risks.

(2) The organisation should systematically appraise its risk exposure, identify risks, and create control measures to deal with those risks. The control measures should be developed in conjunction with the risk identification and assessment process.

(3) The controls should be clearly documented in the financial management practice manual, policies and procedures and employees should receive training in these.

(4) The organisation should conduct appropriate screening of prospective employees for disciplinary and criminal history in addition to conducting referee and qualification checks. These checks should also be conducted before an existing employee is moved or promoted to a high-risk position.

(5) The organisation should conduct appropriate due diligence screening of prospective providers of goods and services. This should include a risk assessment and referee and finance checks.

(6) The organisation should use data analysis techniques as a detection tool, particularly in high risk areas.

(7) Management and employees should share the day-to-day responsibility for implementing and monitoring internal controls. Managers should bear the primary responsibility for leadership and for implementing and monitoring the control systems. Employees should follow and comply with the control systems and report every detected failure of those systems to their managers.

(8) The control systems should incorporate feedback and review functions that evaluate the effectiveness of the organisation's internal controls against updated risk assessments.

(9) The organisation's internal audit program should independently review the adequacy of the control arrangements on a regular basis.

(10) The internal audit function should develop a strategic internal audit plan appropriate to the size and functions of the organisation to provide an overall strategy for the internal audit function for a period of at least one year, and an audit program that sets out the audits it intends to carry out during the year (FPMS section 31).

Additional reading

- CCC Advisory 2017, *Management of public records*, CCC Brisbane
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management: Integrated Framework*, 2004.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Fraud Risk Management Guide*, 2016
- Queensland Audit Office 2012, Auditor-General of Queensland Report 5: 2012 *Results of Audits: Internal control systems*, QAO Brisbane. <www.parliament.qld.gov.au/Documents/TableOffice/TabledPapers/2012/5412T401.pdf >
- Queensland Treasury 2012, *Internal Controls training*. <http://treasury.govnet.qld.gov.au/internal-controls>

Checklist: Internal controls

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

- ☐ Have appropriate internal control measures been implemented to deal with all the identified fraud and corruption risks? (FA Act section 61, FPMS section 8)
- ☐ Is there appropriate separation of duties between officers of the organisation? (FPMS section 8(6))
- ☐ Is the internal control structure included in the organisation's FMPM? (FPMS section 8(5))
- ☐ Does the organisation review its internal controls system regularly enough to cater for changing circumstances? (FPMS section 15(3))
- ☐ Are the delegations, authorities and supervisory roles of management clearly defined? (FPMS (8)(2)(b)(i)
- ☐ Is there an internal audit function? (FPMS section 29.)
- ☐ Does the internal control structure include appropriately qualified officers? (FPMS section 8(2)(b)(ii))

Recommended Best Practice

- ☐ Are there systems or procedures to regularly monitor and evaluate the controls?
- ☐ If there have been any major changes to the organisation structure, functions or operating environment, have internal controls been reviewed for ongoing adequacy?
- ☐ Are the responsibilities for fraud and corruption control clearly documented in organisation policies, procedures and job descriptions?
- ☐ Does the organisation actively involve senior executives and line managers in reviewing operational practices and controls to prevent and detect fraud and corruption?
- ☐ Have all stakeholders been made aware of the risks and organisation control mechanisms?
- ☐ Do the organisation's contracts with suppliers require the supplier and their staff to comply with the organisation's key integrity policies?
- ☐ Are line managers and employees made aware of the content of policies and procedures and controls relevant to their roles and to fraud control?
- ☐ Are the managers aware of their obligation to ensure their staff know and implement the internal controls relevant to their role?
- ☐ Do the employees in these positions consciously accept their control responsibilities?
- ☐ Does each work unit or business process comply with all policy obligations for delegations and organisational review?
- ☐ Does the organisation conduct checks on prospective employees' references, stated qualifications, criminal histories and discipline records?
- ☐ Are organisation delegations routinely reviewed and employees advised of relevant changes?
- ☐ Does the organisation regularly check for duplication, overlap, conflict or lack of coverage that is likely to reduce the effectiveness of the organisation's fraud and corruption controls?
- ☐ Does the organisation implement routine data analytics in areas identified as inherently susceptible to fraud?

- ☐ Are managers and employees consulted about specific investigations which may involve any control lapses in their areas of operation?
- ☐ Do any supervisors affected by changes in controls review the interim or final investigation reports as part of their obligations to understand and apply the anticipated changes?