Understanding Internal Controls

Internal controls feature prominently on an organisation's risk register, yet one of the major weaknesses of AS/NZS ISO 31000:2009 Risk management - Principles and guidelines is the lack of guidance around internal controls and in particular, the different types of controls and how they work to mitigate risks. Tony Harb and Mitchell Morley, risk management, audit and governance specialists from InConsult take a close look at the role of internal controls, the various types and their limitations.

Along with forecasting, planning, organizing, commanding and coordinating, the famous management theorist Henry Fayol identified 'controlling' as one of the six functions of management.

AS/NZS ISO 31000:2009 Risk management - Principles and guidelines defines control as a "measure that is modifying risk" and includes "any process, policy, device, practice, or other actions". The standard also warns that "controls may not always exert the intended or assumed modifying effect". Unfortunately, it does not go further to guide risk owners in better understanding the key attributes of internal controls and their role in the risk management process.

The AS/NZS ISO 31000:2009 definition is a relatively simple one. From an organisational management context, internal audit and COSO ERM framework literature contain more comprehensive definitions of internal control, better highlight control objectives and link controls to helping the organisation achieve its objectives.

Internal Controls

Internal controls are simply processes, policies and procedures, effected by people

that ensure our internal processes, designed to modify risk, work the way we want them to so that we achieve what we want.

An organisation will have hundreds if not thousands of internal controls in place.

Examples of internal controls include separation of duties, authority delegations, policies, procedure manuals, work practices, passwords, account reconciliations, arithmetical accuracy checks, restricted physical access, stock counts, asset counts, budgets, plans etc.

With potentially thousands of different controls, with different levels of effectiveness, it is important to categorise them into different groups to better understand them.

One of the most popular ways of categorising controls is according to "when" they address the risk, error or irregularity.

Preventative Controls

Preventive controls are designed to stop, discourage or pre-empt inappropriate transactions, errors or irregularities before they occur. These are the most desirable as they STOP problems from occurring.

Preventive controls are proactive and emphasize quality as they minimise re-work.

They tend to be more cost-effective than other controls. Preventive controls (or any control) always involve additional processes but the processes are put up front to direct outcomes so things won't go wrong.

Some good examples include documented procedures that clearly describe steps in a process, passwords that prevent access to a system and physical controls over assets such as securely locking up trucks and equipment to prevent theft.

Detective Controls

Detective controls are designed to search for and identify errors on a timely basis after they have occurred.

Detective controls are after-the-fact controls.

Detective controls can also be used to measure the effectiveness of preventive controls.

In some cases, it may not be possible to have a preventative control and so detective controls are the most effective way to manage certain types of risks.

Examples of detective controls include account reconciliations that identify errors, periodic stock counts that identify shortages and errors and secondary authorisations to detect processing errors.

Corrective Controls

Corrective controls are designed to correct errors or risks and prevent the recurrence of further errors.

They begin when undesirable outcomes are detected and keep the "spotlight" on the problem until management can solve the problem or correct the defect.

Examples of corrective controls include quality teams that address ongoing problems to correct processes, thermostats on machines that automatically trigger cooling systems to correct temperature imbalances and insurance programs that recover financial losses to return the insured to the same financial position they were in prior to the loss.

Soft and Hard Controls

Controls may also be soft or hard.

Soft controls are intangible controls that management emphasizes to direct the organization's expectations and behaviour.

Examples of soft controls include management philosophy, operating style, ethics, integrity, attitudes, communication, feedback, training programs and commitment and competency of employees.

Hard controls are visible, traditional internal controls such as documented procedures, reconciliations, formal systems and monitoring outputs.

Manual and Automated Controls

Controls can also be implemented by people manually or by computer systems automatically.

Manual controls are affected by, and rely on, people and are typically independent of IT processes.

Examples of manual controls include approval of manual petty cash forms and manager review of transaction listings.

Automated controls on the other hand rely on computers/technology to identify, prevent or correct errors, variations or

risks. They can be preventive, detective or corrective.

Automated controls can reduce the cost of monitoring as well as lowering processing and compliance costs.

It is important to note that the above attributes of internal controls are not mutually exclusive. i.e. a control can be corrective, hard and manual in nature.

Limitations of Internal Controls

Internal controls have their limitations too. They can be ignored, bypassed, over-ridden, prone to errors, inconsistent and subject to judgement.

Control Effectiveness in Practice

Measuring control effectiveness is critical in the risk management process because the effectiveness of controls will have a direct impact on the level of residual risk.

In NSW, the Independent Commission Against Corruption (ICAC) perceives corruption risk as inherently high in local government. Many, if not most, councils would have all the internal controls suggested by ICAC in place e.g. code of conduct, fraud control plan, risk assessment, internal audit etc.

But the question is not if these controls are in place, but how effective they are. For example:

- A code of conduct that is not communicated to new staff and continually reinforced is not very effective.
- A fraud control plan last updated in 2003 is probably not very effective.
- Risk assessments 'borrowed' from another council that did not involve key people in the process is also unlikely to be very effective.

Bottom line

It is critical that management is honest and realistic when designing, implementing and evaluating the effectiveness of controls and understand exactly how a particular control is addressing the risk. A risk based internal audit program can also provide independent assurance about the effectiveness and efficiency of internal controls.

By better understanding the nature, characteristics and limitations of internal controls, risk owners and management will be well positioned to improve their risk management framework and achieve their objectives.

Tony Harb & Mitchell Morley can be contacted on 02 9241 1344 or tonyh@inconsult.com.au