

Strategies for Improvement

Outputs of the self-assessment process

Scoring the self-assessment

The risk management and control self-assessment matrix (in Volume 2) is divided into 3 major segments that are designed for use by:

- ◆ CEO/senior management/executive teams
- ◆ line managers
- ◆ internal audit.

The matrix is made up of elements (as defined by the BPS), each element is made up of a certain number of components. Components are assessed by reference to a limited number of questions. Each question will be allocated a score depending on the response selected, and an average calculated for that component.

You should insert your responses for each question on the individual response sheet (see example and response sheets in Volume 3). Once all questions are answered, an average should be calculated for each control component on the response sheet.

At the end of the self-assessment process and when all individual response sheets are completed, they should be aggregated and reviewed for any significant differences or inconsistencies. This review could be conducted by the project manager or the whole team may want to be involved. Differences could be the result of very different experiences of internal control or could represent bias or "soft option" responses.

The organisation self-assessment is only of value to an organisation in terms of representing real issues and risks - any failure to grapple with real issues can only represent an increased risk so far as the organisation is concerned. After any differences are resolved, an aggregate average should be calculated for each control component

(see example and aggregate response sheets in Volume 3). In calculating the aggregate averages, all response sheets may be used, or they may be split between different management levels or operational staff levels for comparative purposes.

Organisation profile

Based on the aggregate average for each component, a graphic profile of the organisation performance can be mapped using the Internal Control System Status Report or "wheel" (see page 5, Volume 3). The centre of the "wheel" contains concentric circles marked 1 through to 4. This represents the "basic" to "best practice" continuum on which the aggregated average scores are to be recorded.

Using the "wheel" provided, mark the aggregate average score for each component and shade the area from the centre. Once this is done for all components, it provides an overview of the organisation's performance compared to best practice and the desired organisation position.

There are plans to establish a database to capture and summarise the information recorded on the response sheets. This will allow organisation averages to be calculated automatically, and facilitate the generation of the graphic profile of organisation performance.

Action plan and strategies for improvement

The self-assessment provides a summary of the key strengths in the organisation's application of internal control, and priority areas for performance improvement as a preliminary to the action plan.

The action plan highlights specific actions and strategies for implementation under the priority improvement areas. Identifying the benefits to be gained from implementing the improvements must form part of the overall action plan.

Use the Strategies for Improvement Tool (on pages 19 to 24 in this Volume) to develop strategies tailored for your organisation.

The strategies for improvement are organised under the headings of the four key success factors that are constantly emerging from research at both the local and international levels. These four key success factors are:

- ◆ the leadership of risk management and internal control;
- ◆ the nature of human resource mechanisms that reinforce risk management and internal control;
- ◆ clarity of accountability for risk management and internal control at both the job and process levels;
- ◆ the effectiveness of business and control process supports.

In developing the strategies, the following sources of information have been drawn on:

- ◆ the survey findings;
- ◆ overseas research;
- ◆ expert focus group input (consisting of members of public sector agencies with expertise in risk management and internal control);
- ◆ steering committee comments (comprising representatives of NSW Treasury, the Premier's Department, the Public Employment Office, the Cabinet Office, the Audit Office of New South Wales and Pricewaterhouse Coopers).

Under each key success factor:

- ◆ the strategies have been grouped according to;
- ◆ a goal or outcome statements that represent indicators of best practice;
- ◆ the strategies are followed by the risks associated with failing to achieve in terms of that particular success factor.

The strategies presented here are generic examples of actions that could be taken. It is the responsibility of each organisation to:

- ◆ make their own self-assessment using the matrix and the "wheel";
- ◆ determine where they want to be in terms of best practice using the matrix and "wheel";
- ◆ identify those areas where they have the biggest gap between current and desired C1 practice;
- ◆ focus on the success factors that are most appropriate: refer to cross reference chart of internal control components and success factors on page 25;
- ◆ review the strategies listed to identify those relevant to their organisation;
- ◆ customise the strategies to their particular organisation's situation and need;
- ◆ consider other strategies that may be needed to augment their organisation's approach to improving internal control practices.

The strategies listed here are therefore indicative only; they should not be used without being customised to an agency's needs and they should not be seen as exhaustive. Examples are provided as illustrations only of how the strategies can be operationalised. Strategies can only succeed given the organisation context and the factors that impact on its operations. Time, history, organisation culture, the nature of leadership and management competence within an organisation need to be taken into account in developing strategies, together with such practical issues as the resources (time and funds) that can be made available.

The customised strategies should be signed off by the senior management team and responsibilities assigned against an agreed timeline for their implementation.

Leadership

◆ *Internal control is recognised as a critical component of corporate governance*

- The CEO/senior executives are identified as having primary responsibility for internal control. Internal Control Statement of Responsibility requires sign-off by line management and CEO, all employees are designated with individual responsibility
- Corporate planning integrates corporate objectives, risk management and required internal controls.

◆ *Risk management is valued and exercised as a core competency of the agency*

- Appropriate managers prepare risk management plans linking organisation objectives, risks and controls. These plans encompass financial reporting, compliance and operational risks. Risk management plans are distributed to staff responsible for meeting objectives and/or performing control activities
- Senior management demonstrate risk management competency by reviewing and applying risk management plans, commenting on its importance to both internal and external audit and actively supporting training.

◆ *Corporate culture incorporates risk management and internal control as a key business value*

- Senior executives reinforce the importance of risk management and internal control by integrating it with all corporate governance objectives, for example, by incorporating it into corporate planning and by having a strong Audit Committee with broad mandate

- Senior executives identify and empower effective change facilitators (Internal and/or external) by establishing appropriate role, responsibility autonomy and skills to challenge the organisation
- Strategic objectives are discussed with staff so they understand how they contribute to them and how important it is for any risk to their achievement to be identified and monitored as an integral part of doing business;
- Senior executives communicate a clear message for all staff that internal control is “everyone’s responsibility”;
- Management monitor the effectiveness of communication processes by surveying both content and process against agreed objectives;
- Management regularly communicate and reinforce the importance of internal control. For example, all new policies should refer to the context of internal control and the interdependencies;
- Management demonstrate commitment to maintaining effective internal control, for example, through incorporating the concepts into executive meetings, all HR policies (training, performance assessment, peer group assessment), newsletters, informal feedback, etc in order to better meet individual and agency objectives;
- Establish a code of business conduct/ethics covering the key decision making and action areas of organisation;
- Reinforce requirements of the code of business conduct/ethics in all decision making and actions by having:
 - ◆ Management decisions comply with the letter and spirit of the Code of Conduct;
 - ◆ Code of Conduct reviewed, applied and monitored by CEO/senior executives;
 - ◆ CEO/senior executives communicate the importance of ethical leadership and ensure this is translated into behaviour expected on the job;

- ◆ CEO/senior executives require all decisions to be ethically sound;
- ◆ any possible breaches investigated and actual breaches to code of conduct strongly sanctioned.
- Institute effective performance monitoring so that disciplinary action is a recognised consequence of failure to exercise appropriate internal control
- Expert systems are developed to hold "corporate memory" including users and internal controls.

◆ ***Internal control leadership acts as an effective balance between control and empowerment***

- Define job responsibilities and accountabilities in line with the potential risks to the achievement of agency objectives
- CEO communicates expectations to all staff via Audit Committee and other means.

As such the agency may be caught out and have to engage in 'firefighting', using excessive resources without any longer term benefit

- ◆ Overcontrol / inappropriate controls may be used which adversely affect the responsiveness and flexibility of the agency
- ◆ Internal control practices become outdated with limited account taken of best practice developments.

Key risks associated with ineffective risk management and internal control leadership

- ◆ Breakdowns in internal control prevent the agency from achieving its objectives
- ◆ There is no continuing support for internal control - agency loses a critically important process
- ◆ Risk management and internal control fails to be incorporated in culture and remains an "add on" - with minimal impact
- ◆ Risk management and internal control remains the responsibility of internal audit and /or the CFO
- ◆ Reactive response to potential risks - only "ad hoc" and potentially limited
- ◆ Agency may have limited plans in place to deal with adverse events which could have a significant impact on the agency's operations.

HR Mechanisms used to reinforce Risk Management and Internal Control

- ◆ ***All HR policies (especially hiring, induction, performance management, promotion and reward) reinforce the fact that risk management and internal control are the responsibility of all employees***
 - HR policies emphasise appropriate ethical behaviour and knowledge and experience in relation to managing risk to achieve organisation objectives;
 - New employee induction programs include explaining the agency's commitment to internal control and personal responsibility for action;
 - All HR policies are assessed for their risk elements and appropriate controls established;
 - HR policies emphasise broad 'competencies' relevant to organisation objectives.

Specific examples of HR mechanisms reinforcing internal control are seen most powerfully in the following activities:

- ◆ ***Training programs support internal control best practice***
 - Use training to reinforce and emphasise the ethical approach to operations and compliance with code of conduct;
 - Management and staff are trained in risk assessment and risk management procedures;
 - Train management and staff in benefits of internal control and internal control benchmarks and methodologies and linkage to organisation objectives;

- Train people in necessary job skills prior to appointment.

- ◆ ***Performance evaluation reinforces the organisation's commitment to internal control***

- Build risk management explicitly into both staff and management job descriptions and performance assessment criteria;
- Staff and management are assessed in terms of their performance on assigned internal control responsibilities;
- Effectiveness of risk management monitored at individual level through performance management process.

- ◆ ***Disciplinary action reinforces importance of maintaining effective control procedures***

- Disciplinary action is taken when agreed control / risk management procedures are not adhered to.

Key risks associated with HR mechanisms which do not support risk management and internal control

- ◆ Risk management and internal control not understood by management and staff and therefore not actioned;
- ◆ Risk management and internal control considered unimportant by management and staff;
- ◆ Risk management and internal control not implemented by management and staff;
- ◆ Risk management and internal control remains at theoretical/conceptual/systems level and has no real impact in people's behaviour on the job.

Accountability for Risk Management and Internal Control

◆ ***Responsibility for controlling strategic risks, business processes and compliance processes is clearly defined both at the systems and individual job level***

- Formal policies define internal control processes
- Job descriptions specify individual responsibilities and accountabilities, eg line management sign off a Statement of Responsibility
- Internal audit has a clear defined charter distributed to all executives and staff
- Risks associated with each agency process are clearly identified, documented and controls specified both in a risk management plan and in individual responsibilities
- Effectiveness of risk management within agency processes is monitored at systemic level. At individual level, monitoring is through performance management system
- Procedures are in place for reporting internal control deficiencies and communicated to all staff.

◆ ***Responsibility for risk management and internal control is accepted and acted upon by each individual***

- Consequences for not following internal control processes are clearly defined and consistently applied
- All staff are responsible for reporting internal control weaknesses.

◆ ***Individuals are responsible for proposing improvements to internal control and reporting suspected incidents and unethical behaviour***

- Encourage suggestions for improvement through communication by management, timely evaluation of suggestions and/or some type of incentive system;
- Implement a simple procedure for all staff to bypass the usual communication channels where they need to report suspected incidents or ethical breaches eg whistle blower protection;
- Internal control is independent, yet accountable to CEO and Audit Committee.

◆ ***The organisational structure supports an effective internal control environment***

- The organisational structure (at all levels) is regularly reviewed by management for effectiveness in meeting agency objectives;
- Responsibility for risk management, internal control and internal audit is delegated to an appropriate level and defined within position responsibilities.

Key risks associated with a lack of accountability for risk management and internal control

- ◆ Risk management and internal control is not taken seriously by management and staff - the concepts are never actually incorporated into agency processes;
- ◆ Risk management and internal control procedures which have been established are not followed by management and staff;
- ◆ New ideas about risk management and internal control are rarely suggested;
- ◆ Breakdowns in internal control are not communicated.

Business and Control Process Supports

◆ *An effective internal control system covers all organisational systems ranging from forecasting and planning through operations to monitoring and reporting*

- Audit Committee established, even in absence of a Board;
- Audit Committee accountable for organisation risk management plan from preparation through to monitoring
- Specific high risk issues, for example fraudulent use of resources, misappropriation of cash funds etc are clearly named with employees and environmental scanning processes put in place to monitor incidents.

◆ *A common language and communication supports an effective internal control environment*

- Internal control benchmarks/standards, eg NSW Treasury Best Practice Statement, COSO, CoCo, Cadbury, are adopted to create a common language and framework for best practice internal control
- Use of a common language in relation to risk and control is reinforced through training for all staff and daily use in meetings
- Responsibility for keeping abreast of internal control developments is assigned to appropriate staff and significant developments are communicated to staff on a regular basis.

◆ *Risk management is specifically incorporated into all management planning, resource allocation and control processes*

- Clearly align all functions and tasks to organisation objectives

- Clearly define risk assessment procedures (aligned to corporate objectives) and ensure they are understood by, communicated to and owned by, all employees
- Undertake regular risk assessments
- Produce a comprehensive 'risk management' plan as part of strategic planning
- Take action on a timely basis to eliminate/ reduce adverse impact of identified risks eg included as standing item in management meeting
- Regularly review control processes for effectiveness in eliminating/reducing risks by auditing both processes and outcomes.

◆ *Internal controls are designed around achieving organisation objectives by mitigating risk*

- Controls are risk based, focusing on the right person at the right time (where the risk is greatest) exercising control to mitigate risk
- Controls encompass financial reporting, compliance and operational controls
- Controls are both preventive and detective, anticipating 'off track' performance, and cover both inherent and control risk.

◆ *Ongoing monitoring is incorporated into the overall internal control environment as a dynamic process*

- Monitor performance and effectiveness of the internal control environment in eliminating or reducing the impact of risks on the agency objectives (eg by Audit Committee, internal audit, and all tiers of management and staff on a regular or continuous basis). Critical success factors are needed in monitoring procedures including key risks
- Internal audit functions are co-ordinated with other review functions

- Internal audit reports formally and frequently to CEO
- Monitor changing nature of risks in relation to achievement of overall agency objectives eg addressed in corporate planning
- Establish timely communication process to provide appropriate feedback to managers regarding internal control strengths, weaknesses and deficiencies
- Internal audit focuses on key risks of not achieving strategic objectives and recommendations focus on critical success factors.

◆ ***Information focus on the system and effective communication facilitates achieving objectives***

- Information is captured that relates to financial, compliance and operational objectives and risks
- Information system and technology are linked to corporate objectives
- Information is openly and fully communicated (top down, bottom up and laterally) to facilitate making the right decisions
- Objectives, strategies and risks are communicated to all staff, eg by participation in the development of the corporate plan.

Key risks associated with ineffective business and control process supports

- ◆ Risks are not fully considered
- ◆ Lack of common language makes communication more difficult and less effective
- ◆ The effectiveness of the internal control system is not assessed
- ◆ The benefits or otherwise of changes to the internal control system cannot be determined
- ◆ Changing/new risks are not adequately considered and managed.