June 2017

Guide for Audit & Risk Committees: Compliance Management

What are compliance obligations?

NSW Government Agencies have a wide range of compliance obligations. These include (but are not restricted to):

- laws and regulations
- legal or administrative judgements
- contractual obligations
- agreements with stakeholders
- standards and codes
- Government requirements including policies and procedures

Failure to meet these obligations can have significant repercussions for Agencies including not only legal and financial consequences, but also reputation risk. Failing to demonstrate an active commitment to compliance can undermine an Agency's perceived integrity.

Compliance management system

An active commitment to compliance can be demonstrated through the development and implementation of a Compliance Management System. An effective Compliance Management System will help an Agency to:

- develop and promote a compliance culture that recognises the importance of compliance to the organisation
- identify and meet its specific compliance obligations
- understand its compliance risks including the likelihood of non-compliance and the consequences of non-compliance
- develop, implement and monitor internal controls to address its compliance risks
- assess and improve its compliance performance

There are many guides on the development of an effective Compliance Management System that Agencies can use when developing their own Compliance Management System. A key reference should be the Australian Standard AS/ISO 19600:2015 Compliance Management Systems – Guidelines. Rather than prescribing requirements, the Standard provides guidance to developing a Compliance Management System based on a risk management approach and a commitment to continuous improvement.

It is important to note that there is no single Compliance Management System that will be appropriate for all Agencies. Agencies need to develop and manage a Compliance Management System that best reflects the needs of the Agency. However, some of the elements common to an effective Compliance Management System include:

- Tone at the top – a strong and explicit commitment to establishing and maintaining a compliance culture
- A compliance policy – a statement of the scope of the Compliance Management System and its objectives, together with accountabilities and responsibilities under the system
- Clear and specific allocation of responsibilities for ensuring compliance – clarity about the expectations on individuals within the Agency about their respective compliance obligations
- A mechanism for identifying and understanding compliance obligations – processes are in place to monitor an Agency's compliance obligations and to respond quickly and effectively to meet new compliance obligations

- Communication and training – employees, contractors and other representatives of the Agency are aware of their compliance obligations and have the necessary knowledge and skills to be able to meet those obligations

- A clear process for assessing compliance risk – a periodic (e.g. annual) and specific assessment of the likelihood and consequence of failing to comply with the Agency's obligations that allows the Agency to understand its compliance risk exposure and prioritise resources to best mitigate that exposure

- Actions to address compliance risks – controls have been designed and implemented and are in place to minimise the risk of non-compliance, particularly in areas that have been identified as high risk based on the compliance risk assessment

- Mechanisms for assessing and improving the Agency's compliance performance – not only are instances of non-compliance identified and remedied but the Compliance Management System is routinely reviewed and tested to support its continuous improvement

Role of the Audit & Risk Committee

The Model ARC Charter in TPP 15-03 Internal Audit and Risk Management Policy for the NSW Public Sector requires the Audit & Risk Committee (ARC) to review an Agency's Compliance Management System in order to:

- determine whether management has appropriately considered legal and compliance risks as part of the Agency's risk assessment or management arrangements

- review the effectiveness of the system for monitoring the Agency's compliance with applicable laws and regulations, and associated Government policies.

In addition to raising issues of concern with management as they are identified, the ARC also has a responsibility to include an assessment of the Agency's compliance framework in its annual report to the Agency Head.

Example Checklist for ARCs

An example checklist with questions that the ARC might consider asking of management to test the integrity of the Compliance Management System is provided below. The ARC should tailor the checklist to meet the specific needs and circumstances of the Agency.

Test question	Response
What evidence is there of a strong and explicit commitment to establishing and maintaining a compliance culture?	
Does the Agency have a compliance policy with defined and measurable objectives, indicators and clear accountabilities? Have staff and other relevant stakeholders been made aware of the policy?	
Is the scope of the Compliance Management System clear and appropriate to the Agency?	
Is responsibility for the Compliance Management System clearly assigned within the Agency?	
Does the compliance function of the Agency have appropriate authority and resources?	
How are current and emerging compliance obligations identified and monitored?	
Are identified compliance obligations analysed and is the impact of non-compliance evaluated?	
Is there a specific process for assessing the Agency’s compliance risk?	
As a result of that risk assessment, does the Agency have a sound understanding of its compliance risk exposure?	
Have controls to mitigate the Agency’s compliance risk been identified and implemented?	
How are staff made aware of their current and emerging compliance obligations?	
What mechanisms are there to ensure that staff have the necessary skills and knowledge to meet their compliance obligations?	
Is compliance of outsourced programs and services monitored through third-party performance appraisals and effective contract management?	

Test question	Response
Are there clear and accountable escalation points for non-compliance to be raised?	
Is the Compliance Management System documented and reported on?	
Have previous instances of non-compliance been addressed?	
Are the following activities effectively engaged to support continuous improvement of the Compliance Management System: ▪ Compliance monitoring processes including processes for seeking and receiving feedback ▪ Compliance reporting ▪ Internal audit ▪ Management review ▪ Other review and evaluation mechanisms (describe)	
Are the components of the Compliance Management System communicated, supported, reviewed and revised regularly with a focus on continuous improvement?	