



Title:

Identifying Compliance Risks Guideline

Version	1.3
TRIM file number	09/
Short description	Procedure on the management of compliance within the University.
Relevant to	All employees
Approved by	Vice-Chancellor
Responsible officer	University Secretary
Responsible office	University Secretary
Date introduced	25 May 2009
Date(s) modified	
Next scheduled review date	24 May 2011
Related University documents	Risk Management Policy Compliance Management Procedure
Related legislation	See Legislative Guide
Key words	legal, compliance, risk, legislation,

INTRODUCTION

- 1.1 This Guideline has been prepared to assist staff to complete the compliance section of the Risk Register.
- 1.2 For legislative compliance risks, a Legislative Guide has been prepared that identifies which area of the University is specifically responsible for management of the compliance risk.

STEP 1 – IDENTIFYING COMPLIANCE RISKS

There are three main sources of compliance risk for University centres:

- (1) Internal Compliance - Risks associated with not complying with internal rules, policies and procedures;
- (2) External Compliance - Risks associated with not complying with external laws and regulations.
- (3) Other compliance – Risks associated with the operation of one-off programs or activities in Australia or overseas.

Identifying Internal Compliance Risks

The cover sheet of every rule, policy and procedure lists the 'Responsible Office' (in the case of Academic Regulations, this is always the Deputy Vice-Chancellor (Academic)). This indicates the relevant business centre or committee that has overall compliance management responsibility for that rule, policy or procedure. These Offices are responsible for listing the relevant rule, policy or procedure in their Risk Register. The Risk Register aims to help Responsible Offices to identify strategies to ensure all staff and business centres comply with their responsibilities.

For example, the Division of Human Resources would include a Risk Category: 'Non-compliance with *Equal Opportunity Policy*'. In this case, the Division is responsible for identifying "systems" that will maximise compliance for the whole University, not only the Division of Human Resources.

Identifying External Compliance Risks

The Legislative Guide lists major legislative obligations on the University and the 'Responsible Office' for compliance management. As for internal compliance, the Responsible Office must list this in the risk category eg. "Non-compliance with the *Anti-Discrimination Act*".

Identifying Other Compliance Risks

Other compliance risks will arise where business centres engage in one-off programs or activities eg. conducting a course overseas through a third party provider. These risks are ordinarily identified in the Risk Register attached to the commercial business case or UCPC submission. For example, if a Faculty plans to run a new course in Chile, they will need to identify relevant Chilean and Australian laws with which CSU must comply. These must also be notified to the Manager, Corporate Governance immediately and included in the Legislative Register.

STEP 2 - COMPLETING THE COMPLIANCE SECTION OF THE RISK REGISTER

Once you have identified the compliance risk, the area responsible must then incorporate this in their Risk Register and identify risk management strategies. Remember, the Responsible Office must develop compliance management systems for the WHOLE University – not just their own areas.

Risk Event

Each compliance obligation or right should be listed in the 'Risk Event' column in the Risk Register (for example, Failure to comply with *Anti-Discrimination Act*).

Consequence

The consequence of non-compliance should be listed in the 'Consequence' column (for example, penalty, damage to reputation, individual liability for staff member etc).

Mitigating Action

The 'Mitigating Action' column should record the actions currently in place in the area to manage the relevant compliance obligation (eg. Equal Opportunity Policy, EEO Online Module Training required for all staff, Awareness Raising Bulletins on WNN, Complaints Policy and Procedures etc etc).

Residual Likelihood Rating

The residual likelihood rating is the probability of non-compliance arising in light of the mitigating actions that have been identified. The rating should be determined by reference to the likelihood rating table contained in the Risk Management Policy.

Residual Consequence Rating

The residual consequence rating is the impact arising from non-compliance after taking into account the mitigating actions.

The rating should be determined by reference to the consequence rating table for compliance (see below). Remember, the risk consequence rating must be 'LOW' to meet the University's compliance risk appetite. If the risk consequence rating is above 'LOW', then you should review your mitigation actions to see what else can be done to reduce the risk of non-compliance to 'LOW'. You may need to look at a range of options such as:

- (a) Developing a plain language guide for staff and students on how to comply with the obligation;
- (b) Conducting a regular training and development program that guides staff on how to manage the compliance risks;
- (c) Including awareness raising in induction for all new staff;
- (d) Conducting an awareness program (eg. posters, email updates);
- (e) Obtaining regular certification in writing from staff on compliance (to ensure compliance and alert staff to the importance of the issue);
- (f) Include compliance as an item at staff meetings;
- (g) Set up a special committee with responsibility to manage compliance involving key staff who have the influencing capacity to affect behaviour;
- (h) Have an annual seminar presented by staff from the agency responsible for regulating the area;
- (i) Develop a 'best practice' award where staff are recognised for achievement in compliance;
- (j) Obtain expert advice (eg, Legal Office, Office of Corporate Affairs, external advisor) on compliance strategies;
- (k) Appoint a specific officer as responsible for compliance;

- (l) Conduct regular compliance audits or ask the University Auditor to undertake spot-checks throughout the year and make recommendations;
- (m) Incorporate compliance responsibilities into contracts with third parties.

Standards Australia has published a standard on Compliance Programs that sets out a range of best practice strategies for compliance management. You may wish to consult this Standard in developing your mitigation actions. The Standard can be access online through the Library.

Risk Grade, Mitigation Effectiveness, Early Warning

These columns should be completed in accordance with the Risk Management Policy.

COMPLIANCE RISK CONSEQUENCE RATING

LOW - these risks should be recorded, monitored and controlled by the responsible manager. It is expected that specific responsibility for monitoring and implementing actions to manage these risks is assigned to an officer or group of officers and that this officer or officers have a good working knowledge of the compliance obligation. Actions might include an internal guideline setting out the obligation and a presentation at a staff meeting on the obligation and how it is managed.

MEDIUM - Mitigation actions should be implemented to reduce the likelihood and seriousness of non-compliance. Mitigation actions will depend on the consequences of non-compliance to the Faculty or Division and to the University. In addition to the strategies for low level risks, formalised responsibility for compliance coordination should be identified in the position description of an officer or officers, clear guidelines implemented within the area identifying the nature of the obligations or rights and processes for managing this. Awareness raising strategies should be implemented so all staff are aware of the obligation and its importance. Actions to be identified and endorsed at a Faculty or Divisional level.

HIGH - If uncontrolled, a risk event at this level may have a significant impact on the operation of a budget centre or the University as a whole. Mitigating actions need to be very reliable and should be approved and monitored in an ongoing manner by the responsible Dean or Executive Director. Management responsibility should be included in the position description of an identified officer or officers. Clear succession planning processes must be implemented for those officers. A formal policy and procedure should be developed and approved to ensure compliance at all times. It would be expected that risks at this level are discussed at regular intervals at management meetings within a Faculty or Division. Training must be provided to all staff that have responsibilities in relation to the matter and adequate resources made available to those staff to implement the policy and procedural requirements. Awareness raising exercises should be implemented for all staff. A clear reporting framework should be identified and the policy and procedure should identify clear triggers for reporting where a breach of the obligation is possible. The Vice-Chancellor must be advised immediately of current or emerging risks which have been graded at this level.

EXTREME - Activities and projects with unmitigated risks at this level must be avoided or terminated. This is because risk events graded at this level have the potential to cause serious and ongoing damage to the University, the community or the environment. For obligations listed at Extreme, immediate reporting of current, emerging or continuing risk exposures at this level to the Vice-Chancellor and to the Audit and Risk Committee is mandatory.

Table of amendments

Version number	Date	Short description of amendment