APPENDIX 2

There are significant advantages in undertaking risk assessment at the organisational-unit level where the employee is located.

UNDERTAKING A RISK ASSESSMENT TO DETERMINE RISK OF REPRISALS,CONFLICTS AND ADVERSE CONSEQUENCES

WHO SHOULD UNDERTAKE THE RISK ASSESSMENT?

There are significant advantages in undertaking the assessment at the organisational-unit level where the employee is located. The advantages of this are as follows.

- It can be done quickly without having to go through the processes of being referred to a central unit. If there is some risk of reprisal then this can be recognised and acted upon early.
- Much of the information that will be used to undertake the risk assessment will emanate from line management or the employee. It would be counterproductive to refer matters to a central unit that then has to go back to the line management to find out significant information relevant to the assessment. This would take more time and make the process unnecessarily complex.
- By going through the process of assessment at the line-management level, it would remind line managers of their responsibilities to support and protect reporters, as well as provide some degree of assurance to employees under threat that their interests are being taken seriously.

There are, however, some disadvantages in undertaking the risk assessment at the line-management level. These include

- given that the research findings indicate that the most likely source of reprisals is management itself, it might be a leap of faith to assume that line managers are always going to deal with the risk assessment in a fair and reasonable manner
- risk-assessment processes, by their very nature, require some degree of skill and formality that might not be present at the local-management level
- there is a close nexus between good performance management and the effective handling of employees who come forward with reports. If the report has been triggered by shortcomings in the performance-management process then the direct line manager is clearly not a neutral source of risk-assessment advice.

Whether the risk process is conducted centrally, at the unit level, or some combination of both, it is essential that the reporter be involved in the risk-assessment process.

USEFULNESS OF RISK CHECKLIST

The research included detailed analysis of the factors that are more likely to be present when whistleblowing cases result in adverse consequences for the reporter, compared with when they do not (Brown and Olsen 2008b). These factors are a valuable pointer when thinking about risks of bad treatment (for example, reprisals) to reporters. Note that the risks for reprisals by management and co-workers differ.

Those statistical analyses, however, only indicate factors that correlate with less than optimal outcomes. These correlations should not automatically be interpreted as direct causation. If organisations are to fully utilise risk-management techniques to assist reporters, over time they will build up a bank of agency experience that will enable them to more accurately predict the risks of reprisals. In other words, the factors mentioned are a starting point for thinking about risk rather than being definitive.

In undertaking an initial risk assessment, the usual approach, and the one suggested here, is to set down a list of factors that can be quickly scanned and serve to alert line managers to the key problems, such as

- a specific threat against the internal witness has been received
- the issue reported is serious*
- there is more than one wrongdoer involved in the matter*
- the wrongdoing was directed at the internal witness*
- the internal witness has made a report about a more senior officer*
- the wrongdoing that is the subject of the report is occurring frequently*
- the size of the internal witness's immediate work unit is small*
- the internal witness is employed part-time or on a casual basis*
- a history of conflict with management and supervisors exists
- the internal witness has already disclosed his or her identity or they will become identified when the substance of the report is made known
- there is a history of reprisals in the work unit.

(Derived from Brown and Olsen [2008b:137–64]).*

Agencies that have kept records of their whistleblowing processes might be able to add to this checklist with items specific to that particular organisation.

RISK CHECKLIST AS A FILTER OR PRELIMINARY ASSESSMENT

Another issue for organisations when using a preliminary checklist of factors is to determine whether or not that initial risk assessment is going to be used as a filter, or as the first stage in a more comprehensive risk analysis to be undertaken by a central whistleblower-handling unit. These are issues specific to each organisation and decisions need to be made in the light of the existing risk-management structures and skills of managers.

APPLYING THE RISK-MANAGEMENT STANDARD

As mentioned above, virtually all public sector agencies have adopted risk-management practices as part of their everyday operation. The key documents in this process are

- International Standard ISO31000 (2009). *Risk management standard*
- Standards Australia (2004). HB436:2004 *Risk management guidelines: Companion to AS/NZS4360:2004 Risk management standard.*

The risk checklist described above is not a risk assessment in accordance with the principles of the International Standard ISO31000 (2009), but only a suggested starting point.

The practice and implementation of risk management are almost universal in the Australian public sector. Consequently, it is reasonable to assume that the technical capacity to apply the risk-management process does not need reiterating and only the part of the risk-management process that is directly relevant to reporter reprisals needs to be dealt with here.

DETERMINING APPROPRIATE RISK CRITERIA

A key element that would differentiate whistleblowing from the application of risk management to other topics is the selection of appropriate risk criteria. (There is often

some confusion about the notion of risk criteria. Put very simply, it is the dimension of consequence that can be scaled so as to enable some form of measurement of the risk. In many circumstances, risk criteria are quite obvious—for example, when analysing fraud risks, the usual criteria are financial loss and damage to reputation.) In a whistleblowing context, there could be four risk criteria

- harm to the reporter
- performance/efficiency of the organisation
- resources
- reputation of the organisation.

SETTING ACCEPTABLE LEVELS OF RISK

The whole purpose of undertaking a risk assessment is to make a decision as to what needs to be done. Logic dictates that there will be a level of risk set above which action is taken and below which no action is taken. While this is an issue for each organisation to determine, acceptable risk levels against each criterion could be the following.

- **Harm to the reporter.** Both good management practice and obligations to have a safe workplace would lead to the conclusion that there would be a low threshold of acceptable risk when it comes to harm to people within the organisation. The risk level should comprehend immediate and long-term impacts.
- **Performance/efficiency of the organisation.** With this criterion, organisations do have some room to manoeuvre.
- **Resources.** Similar to the above, most public sector organisations would have some discretion in this regard. A very large public sector organisation, however, would have much greater resources at its disposal to deal with one particular case than a much smaller organisation such as a local government authority.
- **Reputation of the organisation.** Very few organisations welcome adverse media attention and it is generally accepted that the threshold here would be reasonably low.

Ideally, in setting acceptable risk levels, the description of the level should be set in such precise terms that anyone in the organisation is clear as to what is the actual level of acceptable risk

Once this step has been concluded, the remaining steps of the standard should be applied.