

Internal Audit Report

Certificate of Compliance – Process and Controls

Reference:	A101 / P001
Period of review:	March – May 2010
Date of final report:	July 2010
Review Sponsor:	David Yarra, Chief Audit Executive, Office of the Chief Audit Executive
Circulation:	Audit Committee Andrew Harvey, Financial Controller, Financial and e-Solutions group

This report and PricewaterhouseCoopers deliverables are intended solely for the Department of Finance and Deregulation's internal use and benefit and may not be relied on by any other party. This report may not be distributed to, discussed with, or otherwise disclosed to any other party without PricewaterhouseCoopers prior written consent. PricewaterhouseCoopers accepts no liability or responsibility to any other party who gains access to this report.

Glossary

Priority ratings have been assigned to issues raised in this report as follows:

Rating scale for individual findings	
A	Active management required as an extreme priority. Controls are not adequate to address the associated risk.
B	Active management required as a high priority. Controls are not adequate to address the associated risk.
C	Active management required as a moderate priority. Controls are not adequate to address the associated risk.
BPI	Business Process Improvement opportunity. A suggested improvement in efficiency or better practice.

Rating scale for overall report

Control is inadequate			Control is adequate	
E	H	M	L	CC
Extreme priority	High priority	Moderate priority	Low priority	Control Critical Test controls regularly

Note: The overall review rating is the residual exposure to Finance after consideration of all findings highlighted in this report. More detail on the rating scales used throughout this report can be found at Appendix D.

Limitations

Our Internal Audit work was limited to that described in this report and was performed in accordance with International Standards for the Professional Practice of Internal Auditing from the Institute of Internal Auditors. It did not constitute an examination or a review in accordance with generally accepted auditing standards or assurance standards. Accordingly, we provide no opinion or other form of assurance with regard to our work or the information upon which our work was based. We did not audit or otherwise verify the information supplied to us in connection with this engagement, except to the extent specified in this report or our approved objectives and scope.



Table of contents

Glossary	i
1 Introduction	3
2 Summary of findings	4
2.1 Summary of ratings and issues	6
2.2 Controls and gap analysis	7
3 Findings and agreed management actions	9
3.1 Performing reviews over the changes to the CoC Matrix	9
3.2 Monitoring of returned certificates of compliance	9
4 "Better Practice" Improvement Opportunities	12
4.1 Succession and business continuity planning	12
Appendix A Summary of work performed	13
Appendix B Certificate of Compliance – Scope of Work	14
Appendix C Prior Year issues resolution	15
Appendix D Review priority and control rating keys	17

1 Introduction

As part of the 2009/10 Internal Audit Work Plan, PricewaterhouseCoopers (PwC) has undertaken a review of the effectiveness of the processes and controls that Department of Finance and Deregulation (Finance) has in place to provide assurance to the Secretary in relation to the Financial Management and Accountability Act (FMA Act) Certificate of Compliance. The internal audit has focussed on:

- Finance's maintenance of a FMA Act Compliance and Controls Matrix;
- the education and guidance provided to assist in the completion of the Certificate; and
- the identification, documentation and reporting of compliance breaches.

The review did not involve detailed sample testing¹ of transactions. A copy of the approved objectives and scope of this review is attached at Appendix B.

It should be noted that internal Audit is also undertaking reviews of Procurement and updates to application controls in Finance's Financial Management Information System (SAP) and has completed reviews of Cash Management and Special Accounts during the year. These reviews have relevance to Finance's assessment of the internal controls in relation to the Certificate of Compliance for 2009/10.

Background

Chief Executives are responsible for promoting the efficient, effective and ethical use of the Commonwealth resources for which they are responsible. Consistent with this is the responsibility to seek to ensure that their agency complies with the relevant governing legislation and associated policies affecting the financial activities and sustainability of the agency.

The Certificate of Compliance provides a comprehensive overview of each FMA Act Agency's compliance with the Australian Government's financial management framework. It certifies that, based on the agency's internal control mechanisms, management and audit committee advice, except to the extent known and noted, the agency complied with the financial management framework over the previous financial year; is operating within the agreed resources for the current financial year; and has adopted appropriate management strategies for all known risks that may affect the financial sustainability of the agency.

¹ Finance has considered the need for sample testing and has determined no further testing is required in 2010 in light of other internal audit work undertaken during the year and perceived residual risk as described above.

2 Summary of findings

Our review indicates that Finance has processes and controls in place which provide reasonable assurance to the Secretary that an appropriate control framework exists in relation to the preparation of the Certificate of Compliance. Areas where Finance can improve the relevant processes and controls are outlined below.

It should be noted that:

- a whilst this review considers the design of processes and controls it does not confirm that controls operated effectively throughout the year
- b our review was performed prior to the finalisation of the Certificate which is due to be completed in August 2010 no internal audit work on the outcome is currently scheduled.

Key strengths

The review highlighted the following strengths in controls and processes:

- **Prior Years issues resolution:** Finance has implemented all agreed management actions from the 2008/09 Certificate of Compliance report. Refer to Appendix C for details of issues and actions.
- **Continuous improvement:** Finance has implemented an action plan during the financial year to reduce the number of breaches occurring within the Department. The breach reduction strategy was provided to the Financial Audit Sub-Committee on the 24 February 2010 and details the incremental implementation of a number of actions. The control improvements brought about by these actions is only effective from the date of implementation which varies across the activity taken.
- **The Compliance and Controls Matrix and guidance for questionnaires:** In 2006 Finance developed a Matrix detailing each element of the FMA Act and associated requirements. The Matrix incorporates Finance's documented guidance, internal controls and the assurance provided by various parties over the requirements. This Matrix is currently being reviewed and updated every three months or when legislation changes. Requirements within the Matrix are reflected in the tri-annual questionnaire to Business Managers.
- **Update of Chief Executive Instructions:** In 2009 Finance completed the review of the Chief Executive Instructions (CEI's). In 2010 all 53 CEIs have been reviewed by the Procurement Advice and Financial Policy Team and relevant participant Business Areas. The CEIs are a key component of the financial management framework within Finance, and by ensuring they reflect current legislation it will enable greater comfort to be obtained over the completeness of the Certificate of Compliance.
- **Financial sustainability reporting process:** For the 2008/09 year, the Audit Committee was provided with sufficient information in relation to the financial sustainability of the agency to agree the agency was operating within the agreed resources for the current financial year. It is expected that similar reporting to the Audit Committee will occur for the 2009/10 year.

Recommendations for Improvement

The following “C” priority rated finding was identified:

- **Performing reviews over the changes to the CoC Matrix:** In 2009, the Procurement Advice and Financial Policy Team (PAFPT) implemented changes to the Certificate of Compliance procedures to update the Matrix on a regular basis and whenever changes occurred. As noted through testing, the changes are reviewed for accuracy at the time they are made and as part of a tri-annual review. Currently the completeness of the changes to the Matrix is not reviewed against a complete record of changes to legislation or other internal/external guidance.
- **Collation and review of certificates of compliance returned:** At the time of PwC review Finance was not recording return of the CoC in a register. It was noted that returns were maintained in an individual employee email box and hard copies in a folder maintained by the same employee. In addition whilst exceptions were followed up by Finance there was no overarching review planned to determine the reasonableness of responses as a whole.

The following “better practice” improvement opportunity was also identified:

- **Succession and business continuity planning:** Presently the PAFPT have put in place procedures and controls in order to improve the quality of assurance over the Certificate of Compliance.

In order to apply these procedures and controls consistently into future reporting periods, PAFPT have drafted an internal procedures document over the Certificate of Compliance. In order to completely achieve the succession planning objective Internal Audit recommend that PAFPT update this document in the areas of preparation and filing to fully reflect processes and controls in place.

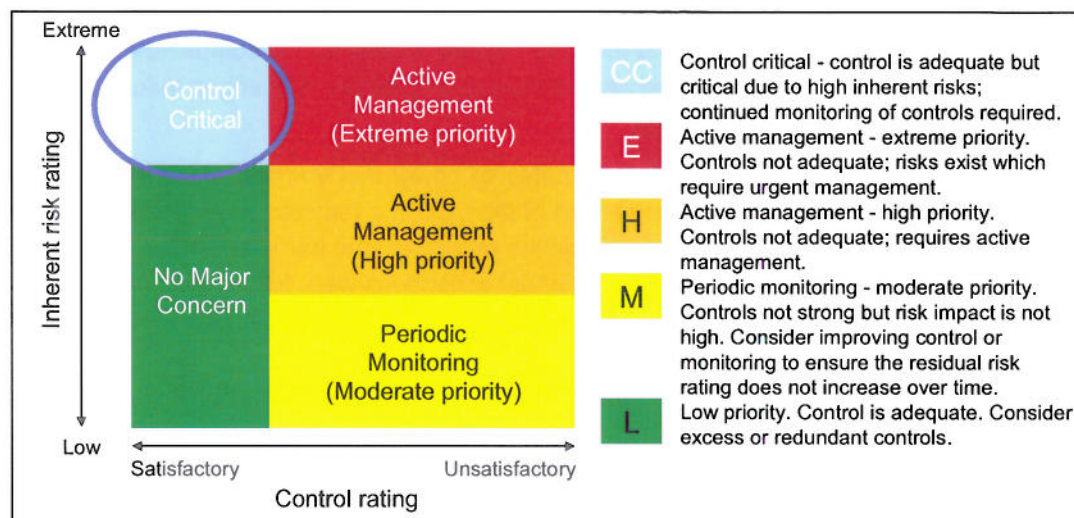
Agreed management actions in response to these findings are summarised within the Controls and Gap Analysis at Section 2.2 of this report. Detailed findings, recommendations and agreed management actions are set out in Section 3.



Mark Ridley
Partner
PricewaterhouseCoopers
20 July 2010

2.1 Summary of ratings and issues

The review has been rated as 'Control Critical Priority' for Finance as illustrated in the diagram below. The two tables below the diagram provide a summary of the individual issues raised in this report. Appendix D provides more detail on the rating scales used throughout this report.



Number of priority issues			
A	B	C	BPI
0	0	2	1

2.2 Controls and gap analysis

We have identified the key controls in place and highlighted control gaps for the Certificate of Compliance process.

Key Controls	Gaps/Issues Noted	Agreed Management Action	Reference/ Priority
Roles and Responsibilities			
<ul style="list-style-type: none"> Roles and responsibilities are defined for the 2009/10 Certificate of Compliance. 	<ul style="list-style-type: none"> No gaps noted 	<ul style="list-style-type: none"> Not applicable 	Not applicable
Planning			
<ul style="list-style-type: none"> Changes to the FMA Act are highlighted in the quarterly questionnaire to alert Business Groups of the items. Compliance and Controls Matrix is regularly updated and reviewed. 	<ul style="list-style-type: none"> No review control to ensure the completeness of the changes to the Matrix or tool to record all changes to legislation or other internal/external guidance for comparison. Internal guidance manual for Certificate of Compliance needs to be updated to ensure consistent continuity of procedures are in place 	PAFPT will maintain a separate register titled 'CoC Legislation Register (CLR)' to record changes to legislation or other internal/external guidance.	3.1 (C) 4.1 (BPI)
Collation of Evidence & Attestation			
<ul style="list-style-type: none"> General Manager signoff required on quarterly questionnaire. Questionnaires are tailored to Divisions. Questionnaire register maintained. Supporting guidance is provided with Questionnaires to Branch Managers 	<ul style="list-style-type: none"> At the time of PwC review a register of returned certificates was not maintained. No overall review of nil breach disclosure was performed to assess appropriateness. 	PAFPT will create a register to track the movements of individual CoC returns from /to Groups.	3.2 (C)
Independent Review			
<ul style="list-style-type: none"> ANAO and Internal Audit reviews of systems and procedures. Record of corrective action taken over breaches. 	<ul style="list-style-type: none"> No gaps noted 	<ul style="list-style-type: none"> Not applicable 	Not applicable
Reporting			
<ul style="list-style-type: none"> Financial Services Branch report to Audit Committee each year on the Certificate of Compliance process. Financial Services Branch Reports to the Audit Committee on the continuity of controls through the course of the FMIS (SAP) implementation. 	<ul style="list-style-type: none"> No gaps noted 	<ul style="list-style-type: none"> Not applicable 	Not applicable

Key Controls	Gaps/Issues Noted	Agreed Management Action	Reference/ Priority
Communication and Education			
<ul style="list-style-type: none"> • Appropriate training for delegates has been conducted • Guidance over the Certificate of Compliance has been provided to Branch Managers 	<ul style="list-style-type: none"> • No gaps noted 	<ul style="list-style-type: none"> • Not applicable 	Not applicable
Review and revision			
<ul style="list-style-type: none"> • Review of Certificate of Compliance processes is conducted by Financial Services Branch. 	<ul style="list-style-type: none"> • No gaps noted 	<ul style="list-style-type: none"> • Not applicable 	Not applicable

3 Findings and agreed management actions

Two findings were identified during the review. The findings and recommended actions are summarised below. An explanation of priority ratings is attached at Appendix D of this report.

3.1 Performing reviews over changes to the CoC Matrix

Observation

In 2009, PAFPT implemented changes to the Certificate of Compliance procedures to update the CoC Matrix on a regular basis and whenever changes occurred.

The changes are reviewed to ensure appropriate, and assessed against the change register for Chief Executive Instructions.

A register for changes to legislation or other internal/external guidance could be maintained, to assess against to ensure the Matrix has included all changes appropriately.

Implication

As changes are performed on an ad hoc basis it is possible that legislative requirements are not fully reflected in the Matrix and therefore that requirements in the tri-annual questionnaire are incomplete. Ultimately omissions or obsolete inclusions in the matrix may lead to reduced comfort over the Certificate of Compliance if not all areas of legislation have been assessed.

Recommendation

That a register of changes to the legislation and guidance be maintained to be used as a completeness check when performing reviews over updates to the Compliance and Controls Matrix.

Agreed Management Action

Priority: C Agreed.

PAFPT will maintain a separate register titled 'CoC Legislation Register (CLR)' to record changes to legislation or other internal/external guidance.

This register will be maintained in the G: drive and reviewed/updated as changes are made to:

- a) FMA legislation
- b) CEIs, delegation instruments and other internal/external guidance.

The controls in the Compliance and Controls matrix will be reviewed and updated three times a year prior to sign-offs being sought in order to reflect the updated legislation and/or other internal/external guidance.

Director, Procurement Advice and Financial Policy Team

31 October 2010

3.2 Monitoring of returned certificates of compliance

Observation

At the time of PwC's review on 7 May 2010 a register of completed CoC's was not being maintained. Furthermore, it was identified that whilst exceptions and breaches were reviewed there was no overall analysis of the completed certificates performed for the purpose of identifying potential omissions.

Risk

There are reporting deadlines in respect of the CoC and reliance placed on the certification by FSB in the annual financial statement process. Failure to identify outstanding certificates in a timely manner impacts the ability to meet reporting deadlines efficiently.

The absence of an overall reasonableness check of the completed CoC's may lead to errors in completion not being identified and inaccurate reporting performed.

Recommendation

A register of completed certificates should be prepared and maintained to monitor the completion of CoC by relevant groups and individuals within the Department.

Secondly at the completion of the certification process a review for reasonableness should be performed across all completed certificates to assess the appropriateness of nil breach responses this review should consist of:

- comparison of responses across groups to identify omissions and unusual trends.
- review of responses against the prior year and the prior year plan to correct.
- review of data with consideration to the internal audit work performed under the 2009 / 2010 to identify if observations from those reviews are correctly reflected in the certificates.
- consideration of the absence of sample testing over certificate compliance in the 2010 financial year.

Agreed Management Action

Priority: C Agreed.

PAFPT will create a register to track the movements of individual CoC returns from /to Groups.

PAFPT email box will be used to send out and receive CoC returns and all electronic documents including emails will be held in a dedicated folder.

The Records Register will be updated to reflect:

- a) the date/s the CoC questionnaire returns is/are sent to Groups
- b) the date/s the CoC matrix is/are sent to Specialist Teams
- c) the return dates of the returns from each Group or team
- d) comments including time extension/s given to Groups and Teams in providing responses.

Formal review of the responses will continue and feedback on the questionnaires will be sought from all groups. The Assistant Secretary, Financial Services Branch will consider the need for detailed sample testing for the annual certificate of compliance process and provide advice to the Audit Committee and Chief Audit Executive.

Director, Procurement Advice and Financial Policy Team

31 July 2010

4 “Better Practice” Improvement Opportunities

The following “Better Practice” improvement opportunity was also identified:

4.1 Succession and business continuity planning

The Procurement Advice and Financial Policy Team have put in place procedures and controls in order to improve the quality of assurance over the Certificate of Compliance.

To ensure consistent application of procedures and to address business continuity and succession planning risks, PAFPT have drafted an internal procedures document over the Certificate of Compliance.

Internal Audit has reviewed this draft document and has identified further inclusions to improve the completeness of the document.

Under Preparation

- 1 When the Matrix is/will be updated;
- 2 Who updates the Matrix;
- 3 How is the Matrix updated i.e. what documents need to change to be reflected in the
- 4 Matrix;
- 5 Who reviews the changes and how do they review the changes;
- 6 How version control is maintained of the documents.

Under Filing

- 1 Note procedures over maintenance of the questionnaire register and include the checklist to be applied for when questionnaires are returned (e.g. where they are located, guidance notes etc).

Agreed Management Action

Item is noted and will be considered when the procedures and controls are next reviewed and updated.

Director, Procurement Advice and Financial Policy Team

Appendix A Summary of work performed

A summary of the work performed against each scope point is outlined in the table below.

Ref	Review scope point	Summary of work performed
1.	Review the Compliance and Controls Matrix that Finance maintains for the Certificate of Compliance.	<ul style="list-style-type: none"> Reviewed controls over the updates to the Compliance and Controls Matrix and the Certificate of Compliance quarterly questionnaire to ensure controls are appropriate.
2.	Update the Matrix (controls and process) through consultation with the Financial Services Branch and Group Finance Managers.	<ul style="list-style-type: none"> Held discussions with the Procurement Advice and Financial Policy team to determine controls and procedures in place over the Certificate of Compliance.
3.	Document and review the processes and controls Finance has in place to educate and promote the importance of the Certificate and to provide guidance to the staff as to the requirements of the Certificate of Compliance.	<ul style="list-style-type: none"> Held discussions with the Procurement Advice and Financial Policy team to identify the processes and controls in place over the promotion and education of the Certificate of Compliance.
4.	Review the processes and controls Finance has in place to identify, record and report on breaches relevant to the Certificate of Compliance.	<ul style="list-style-type: none"> From above discussions and review of evidence, we documented and reviewed the processes and controls Finance has in place to identify record and report on breaches relevant to the Certificate of Compliance.
5.	Where it appears as though controls are poorly designed or implemented, conduct reasonable enquiries to gain insight into the exposure arising.	<ul style="list-style-type: none"> Performed a gap analysis over current procedures and documented the potential risk arising from the control weakness and provided practical recommendations to improve processes and controls.

Appendix B Certificate of Compliance – Scope of Work

Objective

The objective of this review is to report to the Chief Audit Executive annually on the extent to which Finance has effective processes and controls in place to provide assurance to the Secretary in relation to the Certificate of Compliance (required by Finance Circular 2008/04).

Scope and Approach

We will consult with the CFO and Financial Controller to validate our proposed approach and to listen to any concerns or areas of focus they raise, noting that in the first year both the CFO and Financial Controller are new to their positions and may have different preferred approaches to previous work undertaken.

Specifically our approach will be to:

- Review the Compliance and Controls Matrix that Finance maintains for the Certificate of Compliance.
- Update the Matrix (controls and processes) through consultation with the Financial Services Branch and Group Finance Managers.
- Through discussion, observation and review of evidence we will document and review the processes and controls Finance has in place to educate and promote the importance of the certificate and to provide guidance to staff as to the requirements of the Certificate of Compliance.
- Through discussion, observation and review of evidence we will document and review the processes and controls Finance has in place to identify, record and report on breaches relevant to the Certificate of Compliance.
- Where it appears as though controls are poorly designed or implemented, conduct reasonable enquiries to gain insight into the exposure arising.
- Provide practical recommendations to improve processes or controls.
- Provide a view to the CAE on the extent to which Finance's processes and controls are effective in this respect.

Limitations

None specifically noted

Appendix C Prior Year issues resolution

Four findings were identified last year and the following actions have been implemented in the current year.

Prior Year finding	Rating	Observation	Prior Year finding	Rating	Observation
3.1	B	<ul style="list-style-type: none"> • Certificate of Compliance Matrix was not regularly updated to reflect current requirements and controls 	<ul style="list-style-type: none"> • Changes to Finance's Financial Management Framework may not be incorporated into Matrix and therefore not covering all required areas 	<ul style="list-style-type: none"> • The Compliance and Controls Matrix will be updated to reflect the changes to Finance CEI's and guidance; and the operational changes, such the implementation of the financial management system and changes to the Internal Audit arrangements. 	<ul style="list-style-type: none"> • The revised Matrix has been completed and is being used from February 2010. PAFPT will maintain this document with regular updates (3 monthly or as legislation is changed to ensure accuracy is maintained). The Matrix has been linked to the SES Questionnaire which will also ensure the Questionnaire is updated in line with legislative changes.
3.2	B	<ul style="list-style-type: none"> • CEI review to update to current procedures has not been completed. 	<ul style="list-style-type: none"> • Without updating of Chief Executive Instructions Finance's financial management framework may not be incorporating all applicable controls and processes, and this may limit the effectiveness of the Certificate of Compliance process. 	<ul style="list-style-type: none"> • The Financial Services Branch will update the Chief Executive Instructions in accordance with current legislation to ensure that processes and procedures are covering all legislative requirements. 	<ul style="list-style-type: none"> • The CEI Review is complete. All 53 CEIs have been reviewed by the Procurement Advice and Financial Policy Team and relevant participant Business Areas. The final 20 documents were submitted to the GM, FeSG in the week commencing 25 January 2010.

Prior Year finding	Rating	Observation	Prior Year finding	Rating	Observation
3.3	C	<ul style="list-style-type: none"> Inconsistencies in the processes between Business Groups for the preparation of the Quarterly Questionnaire. 	<ul style="list-style-type: none"> Increased risk of inconsistencies between Groups in the quality of data collected and reviewed for the Certificate of Compliance. 	<ul style="list-style-type: none"> Guidance documentation will be created to enable appropriate response to the quarterly General Manager questionnaire. This will ensure that General Managers and Finance Managers are aware of the level of supporting documentation and delegate signoff required and ensure consistency across the Department in respect to the Certificate of Compliance. Formal review of the responses will continue and feedback on the questionnaires will be sought from all groups 	<ul style="list-style-type: none"> The Certificate of Compliance review has been completed and the new version of the questionnaire focussing on the FMA Framework has been developed. A paper has been prepared for Executive Board and Audit Committee, with the new process to commence in late February for the 8 months to 28 February 2010.
3.4	C	<ul style="list-style-type: none"> Internal Audit have not completed a program of sample testing to support the process and provide assurance to the Audit Committee over the Certificate of Compliance. 	<ul style="list-style-type: none"> By not performing sample testing it will lead to increased risk of non-compliance not being reported through the Certificate of Compliance process. 	<ul style="list-style-type: none"> Internal Audit have not completed a program of sample testing to support the process and provide assurance to the Audit Committee over the Certificate of Compliance. 	<ul style="list-style-type: none"> By not performing sample testing it will lead to increased risk of non-compliance not being reported through the Certificate of Compliance process.

Appendix D Review priority and control rating keys

The keys used in this report are based on the Finance Risk Management Framework for inherent risks. Likelihood involves an assessment of the probability or frequency of occurrence of a risk event.

Likelihood	Likelihood of occurrence
Rare	The event type would occur only in exceptional circumstances and has not occurred within Commonwealth Government.
Unlikely	The event type could occur but has not occurred in Finance before.
Average	The event type might occur or has occurred at least once within Finance.
Likely	The event type will probably occur or has occurred in Finance within the last two years.
Almost certain	The event type has occurred within the last 12 months or is expected to occur.

Impact involves the consequences of a risk event, and may be in terms of, for example, financial or human cost, business disruption, environmental damage or damage to reputation. Each consequence/impact can be rated, in terms of its severity.

Impact	Consequence/impact area				
	Financial	Human resources	Business interruption	Outputs	Integrity/ reputation and image
Insignificant	Up to \$100K	First Aid. Leave of absence.	Loss of service capability for up to half a day.	Up to 1% impact on targets.	Internal impact only.
Minor	Up to \$500K	Injury to staff. Temporary loss of key staff.	Loss of service capability for up to two days.	Up to 2% impact on targets.	Adverse comments in local press.
Medium	Up to \$5M	Major injury to staff. Permanent loss of key staff.	Loss of service capability for up to one week.	Up to 5% impact on targets.	Senate Estimates. Other external scrutiny, ANAO, national media. Moderate damage to Finance's reputation.
Major	Up to \$20M	Permanent injury to multiple staff. Loss of critical mass of staff.	Loss of service capability for up to one month. Interruption of two days during Budget. Serious medium term business/environmental effects	Up to 10% impact on targets.	Questions in Parliament. External scrutiny. Serious public, political and/or media outcry.

Impact	Consequence/impact area				
	Financial	Human resources	Business interruption	Outputs	Integrity/ reputation and image
Extreme	Above \$100M.	Multiple deaths of staff. Loss of critical mass of key staff.	Loss of service capability for more than one month. Inability to get Budget completed in timeframe. Very serious long term effects on Department's business.	Greater than 10% impact on targets.	Royal Commission. Judicial inquiry. Other form of Parliamentary inquiry. Possible litigation. Very serious legislative non-compliance.

The intersection of the likelihood and consequence ratings determines the overall inherent risk rating as shown in the table below.

Likelihood	Impact				
	Extreme	Major	Medium	Minor	Insignificant
Almost certain	Extreme	Extreme	High	Significant	Moderate
Likely	Extreme	High	Significant	Moderate	Low
Average	High	High	Significant	Moderate	Low
Unlikely	High	Significant	Moderate	Low	Low
Rare	Significant	Moderate	Low	Low	Low

From this, a level of inherent risk can be determined using the table below.

Level of risk	Description
Extreme	Immediate action required. Move resources from other areas.
High	Action required. Prioritise resources to complete as soon as possible.
Significant	Action required as soon as resources become available, include as a priority on work plans.
Moderate	No immediate action required but to be scheduled for action as part of program or business plan.
Low	No action required but monitor for worsening of the risk.

We then assess the effectiveness of controls that management have in place to manage the risk according to the table below.

	Rating*	Description
Satisfactory	Excellent	Controls have reduced the level of risk to an acceptable level (designed appropriately). Controls are in operation, applied consistently, documented, communicated and monitored.
	Good	Controls have reduced the level of risk to an acceptable level. Controls are in operation, applied consistently, documented, communicated and monitored although minor improvements could be made.
Unsatisfactory	Incomplete	Control is designed to only partially address the risk. Control documentation/communication and/or application require improvement.
	Unsatisfactory	Control is poorly designed and does not fully address the risk. Documentation/communication and/or application need improvement.
	Poor	Control is poorly designed and does not address the risk. Both control documentation/communication and application need improvement.

Residual risk is the level of risk faced after considering the controls in place. Residual risks are rated on the same likelihood and consequence/impact ratings as inherent risks above but are then considered in conjunction with the adequacy of controls. Based on the level of residual risk, management can prioritise the allocation of resources to address these risks through mitigating actions or investments in improving controls. Or areas where management should continue to test controls where residual risks are low, but without the controls, inherent risk would be high – that is, areas where controls are critical, as illustrated in the following diagram:

