2015 (No. 26)

PARLIAMENTARY STANDING COMMITTEE OF PUBLIC ACCOUNTS

REVIEW OF AUDITOR-GENERAL'S SPECIAL REPORT NO.95: *FRAUD CONTROL*

MEMBERS OF THE COMMITTEE

LEGISLATIVE COUNCIL	HOUSE OF ASSEMBLY
Hon Ivan Dean MLC (Chair)	Mr Scott Bacon MP
Hon Ruth Forrest MLC	Ms Sarah Courtney MP (Deputy Chair)
Hon Adriana Taylor MLC	Mrs Joan Rylah MP

CONTACT INFORMATION

Post	Public Accounts Committee Legislative Council Parliament House Hobart TAS 7000
Telephone	03 6212 2300
Facsimile	03 6212 2345
Email	pac@parliament.tas.gov.au
Website	www.parliament.tas.gov.au/ctee/Joint/pacc.htm

Table of Contents

ABBREVIATIONS LIST

DHHS	Department of Health and Human Services • AT - Ambulance Tasmania • HT - Housing Tasmania • LGH - Launceston General Hospital
DoE	Department of Education
DPEM	Department of Police and Emergency Management
DPIPWE	Department of Primary Industries, Parks, Water and Environment • ST - Service Tasmania
TFS	Tasmania Fire Service
UTAS	University of Tasmania

CHARTER OF THE COMMITTEE

The Public Accounts Committee (the Committee) is a Joint Standing Committee of the Tasmanian Parliament constituted under the *Public Accounts Committee Act 1970*.

The Committee comprises six Members of Parliament, three Members drawn from the Legislative Council and three Members from the House of Assembly.

Under section 6 of the *Public Accounts Committee Act 1970* the Committee:

- must inquire into, consider and report to the Parliament on any matter referred to the Committee by either House relating to the management, administration or use of public sector finances; or the accounts of any public authority or other organisation controlled by the State or in which the State has an interest; and

- may inquire into, consider and report to the Parliament on any matter arising in connection with public sector finances that the Committee considers appropriate; and any matter referred to the Committee by the Auditor-General.

RECOMMENDATIONS

Based upon its findings from the follow-up review of the Auditor-General's Special Report 95: *Fraud Control*, the Committee recommends that:

1. All entities introduce a formal mechanism to ensure the future timely review and implementation of the Auditor-General's recommendations;

Department of Health and Human Services (DHHS)

2. The DHHS fully implements recommendation 9 to ensure that senior managers' statements of duties include fraud management as a required responsibility;

Tasmanian Fire Service (TFS)

3. The Department of Police and Emergency Management (DPEM) ensures that the TFS fully implements outstanding recommendations, as detailed in Table 4; and

Service Tasmania

4. The Department of Primary Industries, Parks, Water and Environment (DPIPWE) ensure Service Tasmania implements recommendation 9 to ensure that senior managers' statements of duties include fraud management as a required responsibility.

1 INTRODUCTION AND CONDUCT OF REVIEW

1.1 The Auditor-General's Special Report No. 95: *Fraud Control* (the Report) was tabled in both Houses of Parliament on 15 March 2011.

1.2 The Committee resolved, of its own motion, to review and follow-up on the findings and the implementation of the recommendations of the Report.

1.3 The Report presented the results of a performance audit which examined the effectiveness of fraud control strategies in selected State entities.

TERMS OF REFERENCE

1.4 The Committee's terms of reference were to follow-up on the findings and the implementation of the recommendations of the Report and report to both Houses of Parliament.

CONDUCT OF THE REVIEW

1.5 On 20 August 2014 the Committee received a briefing from the Auditor-General on the Report.

1.6 The Committee resolved to undertake a follow-up examination of the Report on 3 September 2014.

1.7 The Committee developed and distributed a questionnaire to the relevant State entities.

1.8 The purpose of the questionnaire was to determine the action taken by the State entities to implement the recommendations contained within the Report.

1.9 The questionnaires were forwarded to the State entities on 21 October 2014 with the last questionnaire response received on 23 December 2014. The completed questionnaires are attached at Appendix 1.

1.10 The Committee resolved on 10 February 2015 to hold public hearings.

1.11 Representatives of each of the relevant State entities attended public hearings held on 11 March 2015. The Hansard transcript of the hearings is attached at Appendix 2.

1.12 At the hearings the DHHS and DoE agreed to review the questionnaires they had submitted to the Committee and update them to reflect the current position of the Departments. The revised questionnaires are attached at Appendix 3.

2 SPECIAL REPORT NO.95 *FRAUD CONTROL* – AUDIT BACKGROUND AND FINDINGS

2.1 This chapter presents an overview of the background to, and the key findings of the Audit.

AUDIT OBJECTIVES

2.2 The objective of the Audit was to assess the effectiveness of fraud management strategies in selected State entities.

2.3 The Audit scope was concerned with:

- Development and implementation of fraud control strategies;
- Relevant preventative and detective controls for procurement, accounts management, cash handling, corporate credit cards, payroll and IT systems;
- Controls, strategies and policies; and
- The period between July 2009 and October 2010.

2.4 The following State entities were involved in the Audit:

- Department of Health and Human Services (DHHS):
    - Housing Tasmania (HT)
    - Ambulance Tasmania (AT)
    - Launceston General Hospital (LGH);
- Department of Education (DoE);
- Department of Primary Industries, Parks, Water and Environment (DPIPWE):
    - Service Tasmania (ST);
- Tasmania Fire Service (TFS); and
- University of Tasmania (UTAS).

2.5 The aim of the audit criteria developed for the Audit was to address the following effectiveness aspects:

- Does a suitable fraud management strategy exist; and
- Do internal controls prevent and detect fraud?

AUDIT CONCLUSIONS

2.6 The main conclusions of the Report are outlined below.

2.7 The Audit concluded common findings in the areas of:

- General fraud awareness;
- Employment screening;
- Fraud reporting mechanisms;
- Personnel rotation policies;
- Fraud risk assessment; and
- Management accountability.

2.8 The Audit concluded that:

- As a result, attention needs to be paid in varying degrees to the organisational culture at all entities to improve the effectiveness of the fraud prevention and detection mechanisms currently in place.

AUDIT FINDINGS

2.9 In examining the effectiveness of fraud control strategies the Report paid particular attention to:

- The comprehensiveness of fraud control plans; and
- Staff awareness of fraud and fraud control.

2.10 The following Table 1 summarises the Audit findings in the area of planning for fraud control.

Table 1: Findings – planning for an anti-fraud culture[1]

Fraud Control Planning	**DoE**	**DHHS**	**TFS**	**ST**	**UTAS**
Definition of fraud and statement of attitude	✓	✓	×	×	✓
Code of conduct	✓	✓	✓	✓	×
Fraud control planning and review	×	✓	×	×	×
Fraud Control Officer appointed	✓	✓	×	×	✓
Internal audit activity	✓	✓	×	✓	✓

✓ Satisfactory level of compliance

× Recommendation made

[1] Auditor-General Special Report No.95 Fraud Control p.25

2.11 The following Table 2 summarises the Audit findings in the area of controls designed to create the right culture to prevent and detect fraud.

Table 2: Findings – creating the right culture to prevent and detect fraud[2]

Fraud prevention and detection	**DoE**	**DHHS**	**TFS**	**ST**	**UTAS**
Fraud awareness	×	×	×	×	×
Management accountability	×	×	×	×	×
Fraud risk assessment	✓	×	×	×	✓
Personnel rotation and leave management	✓	×	✓	×	×
Employment screening	×	×	×	×	×
Mechanisms for reporting suspected fraud	✓	✓	×	✓	✓

✓ Satisfactory level of compliance

× Recommendation made

[2] *Ibid* p. 28

2.12 The following Table 3 summarises the Audit findings in the area of whether internal controls prevent and detect fraud.

Table 3: Findings – adequacy of internal controls[3]

Control Area	DoE	DHHS	TFS	ST	UTAS
Cash	✓✓✓	✓✓✓	✓	✓✓✓	✓
Corporate Card	✓	✓✓	✓	✓✓✓	✓✓✓
IT	✓✓	✓	✓	✓	✓✓
Expenditure and procurement	✓	✓	✓	✓✓	✓✓
Payroll	✓✓	✓✓	✓✓✓	✓✓✓	✓✓✓
Receipts and receivables	✓✓	✓✓	✓✓✓	✓✓✓	✓✓✓

✓✓✓	Internal controls were well designed and compliance was satisfactory
✓✓	Internal controls were well designed but compliance needs minor improvement
✓	Either internal control design needs improvement or compliance needs major improvement
×	Control design needs major improvement

AUDIT RECOMMENDATIONS

2.13 The Auditor-General made 33 recommendations in his Report based upon his findings. The status of implementation for each of the recommendations has been assessed by the Committee following the return of a questionnaire by each entity and evidence provided at the hearings.

[3] *ibid* p.35

3 COMMITTEE FINDINGS

3.1 The Committee's findings on the status of the implementation of audit recommendations, as detailed in Table 4, are based on the questionnaires completed by the entities and upon evidence provided at hearings held on 11 March 2015. The questionnaires are attached at Appendix 1 and 3. The Hansard transcript of evidence is attached at Appendix 2.

Table 4: Findings – implementation of audit recommendations

		Committee Findings				
Recommendation No:	**Auditor-General's recommendation**	**DoE**	**DHHS**	**TFS**	**ST**	**UTAS**
1	TFS and ST should: • Adopt a fraud definition that aligns with the definition of fraud in either AS 8001-2008 or the Commonwealth Fraud Control Guidelines, develop a statement of attitude to fraud, communicate the fraud definition and statement of attitude to fraud to all employees. • Develop a statement of attitude to fraud. • Communicate the fraud definition and statement of attitude to fraud to all employees.	●	●	×	✓	●
2	UTAS should develop a Code of Conduct that defines expected behaviour for all employees.	●	●	●	●	×
3	TFS and ST should develop comprehensive Fraud Control Plans that address specific fraud risks relevant to them.	●	●	×	✓	●

✓ Recommendation implemented
× Recommendation not implemented
● Not applicable to this entity

Table 4: Findings – implementation of audit recommendations (continued.)

		Committee Findings				
Recommendation No:	**Auditor-General's recommendation**	**DoE**	**DHHS**	**TFS**	**ST**	**UTAS**
4	All entities should review and amend their Fraud Control Plans at appropriate intervals, as a minimum, once every two years.	✓	✓	×	✓	✓
5	UTAS should promptly implement internal audit's recommendations.	●	●	●	●	✓
6	TFS and ST should consider assigning the role of Fraud Control Officer to manage their exposure to this risk.	●	●	×	✓	●
7	TFS should revise its decision to not have an internal audit function.	●	●	×	●	●
8	All entities should introduce mechanisms to ensure that all employees have a general level of fraud awareness that is appropriate for their level of responsibility.	✓	✓	✓	✓	✓
9	All entities should ensure that senior managers' statements of duties include fraud management as a required responsibility.	✓	×	×	×	×
10	TFS, LGH, AT, HT and ST should evaluate all internal and external risks pertaining to the entity, particularly those relating to fraud, and amend the current risk register accordingly.	●	✓	✓	✓	●
11	All entities should develop a policy of personnel rotation and ensure that, while employees are on leave, another employee acts in their place.	✓	✓	✓	✓	✓
12	All entities should perform police checks for senior or high risk positions and document background checks from previous employers.	✓	✓	✓	✓	✓

✓ Recommendation implemented

× Recommendation not implemented

● Not applicable to this entity

Table 4: Findings – implementation of audit recommendations (continued.)

		Committee Findings				
Recommendation No:	**Auditor-General's recommendation**	**DoE**	**DHHS**	**TFS**	**ST**	**UTAS**
13	TFS should develop an alternative reporting mechanism and communicate this mechanism to staff, via a Fraud Control Plan.	●	●	×	●	●
14	All entities should communicate their formalised reporting mechanisms to staff more effectively.	✓	✓	✓	✓	✓
15	DoE should improve corporate card controls by tightening relevant administrative processes.	✓	●	●	●	●
16	DoE should develop and implement: • An IT security plan that covers all aspects of the IT environment, particularly those aspects that relate to fraud prevention and detection. • A regular schedule for testing backups.	✓	●	●	●	●
17	DoE should: • Tighten controls surrounding payment authorisation. • Ensure that all exception reports produced are properly reviewed and that an appropriate audit trail exists in the expenditure and procurement areas.	✓	●	●	●	●
18	DoE should: • Ensure that all exception reports produced are properly reviewed and retained in the payroll area. • Develop a termination checklist to ensure employees' access privileges are removed.	✓	●	●	●	●

✓ Recommendation implemented
× Recommendation not implemented
● Not applicable to this entity

Table 4: Findings – implementation of audit recommendations (continued.)

		Committee Findings				
Recommendation No:	**Auditor-General's recommendation**	**DoE**	**DHHS**	**TFS**	**ST**	**UTAS**
19	DoE should compare actual cash receipts to budgeted cash flow in all areas so that variances are promptly identified and investigated appropriately.	✓	●	●	●	●
20	DHHS should improve: • Corporate card controls by tightening relevant administrative processes, particularly in relation to employee location records and cancellation of corporate cards belonging to former employees. • Compliance with the reconciliation and authorisation controls in the corporate card area.	●	✓	●	●	●
21	DHHS should: • Develop an IT security plan and password policy that cover all aspects of the IT environment, particularly those aspects that relate to fraud prevention and detection. • Ensure that, where appropriate, computers automatically time-out. • Develop a regular schedule for testing backups • Improve controls to ensure that access accounts belong to current employees and reflect current roles at HT and LGH. • Ensure that employees use a unique user ID and password to access all systems and improve server room access controls at AT.	●	✓	●	●	●

✓ Recommendation implemented

× Recommendation not implemented

● Not applicable to this entity

Table 4: Findings – implementation of audit recommendations (continued.)

		Committee Findings				
Recommendation No:	**Auditor-General's recommendation**	**DoE**	**DHHS**	**TFS**	**ST**	**UTAS**
22	DHHS should: • Ensure that the lack of documentation in relation to creditor changes prior to April 2010 is investigated. • Improve internal control at HT to ensure that all invoices are authorised. • Ensure that all orders are properly documented at LGH, possibly by completing implementation of the electronic requisition request process. • Review processes at AT to ensure that initiation and authorisation are independent.	●	✓	●	●	●
23	DHHS should ensure that: • All exception reports produced are properly reviewed and retained in the payroll area. • All changes to the payroll database, such as appointments, terminations and changes in pay are reviewed by independent officers in the Pay and Personnel Unit.	●	✓	●	●	●
24	LGH should ensure that there is appropriate segregation of duties.	●	✓	●	●	●

✓ Recommendation implemented
× Recommendation not implemented
● Not applicable to this entity

Table 4: Findings – implementation of audit recommendations (continued.)

		Committee Findings				
Recommendation No:	**Auditor-General's recommendation**	**DoE**	**DHHS**	**TFS**	**ST**	**UTAS**
25	The Department of Primary Industries, Parks, Water and Environment should develop and implement: • A termination checklist that requires notification of employee separations to IT services in a timely manner. • A password policy that considers current best practice.	●	●	●	✓	●
26	ST should ensure that an appropriate audit trail exists to support information provided in monthly budget variance reports.	●	●	●	✓	●
27	TFS should: • Ensure that all bank reconciliations are properly reviewed. • Improve the strength of electronic fund transfer (EFT) controls.	●	●	✓	●	●
28	TFS should ensure: • Compliance with the segregation of duty control in the corporate card area. • Cancellation of corporate cards for terminating employees.	●	●	✓	●	●

✓ Recommendation implemented
× Recommendation not implemented
● Not applicable to this entity

Table 4: Findings – implementation of audit recommendations (continued.)

		Committee Findings				
Recommendation No:	**Auditor-General's recommendation**	**DoE**	**DHHS**	**TFS**	**ST**	**UTAS**
29	TFS should: • Develop a password policy that considers current best practice. • Improve server room access controls. • Develop a regular schedule to test backups.	●	●	×	●	●
30	TFS should: • Improve internal control compliance in the expenditure and procurement areas. • Improve the segregation of duties in relation to entry and payment of invoices in the Finance system. • Update the financial delegation register. • Ensure that all exception reports produced are properly reviewed and retained in the expenditure and procurement areas.	●	●	✓	●	●
31	UTAS should improve system design to better assist in the performance of bank reconciliations.	●	●	●	●	✓

✓ Recommendation implemented
× Recommendation not implemented
● Not applicable to this entity

Table 4: Findings – implementation of audit recommendations (continued.)

		Committee Findings				
Recommendation No:	**Auditor-General's recommendation**	**DoE**	**DHHS**	**TFS**	**ST**	**UTAS**
32	UTAS should: • Develop a password policy that considers current best practice. • Ensure that computers automatically lock when left unattended.	●	●	●	●	✓
33	UTAS should review changes to the creditor master file on a regular basis and ensure that an appropriate audit trail exists.	●	●	●	●	✓

✓ Recommendation implemented

× Recommendation not implemented

● Not applicable to this entity

3 Committee Findings

DEPARTMENT OF EDUCATION

3.2 The Committee finds that all of the recommendations made by the Auditor-General following the performance review of fraud control within the DoE have been implemented.

3.3 The Committee notes progress made in relation to the DoE's corporate card procedures.

DEPARTMENT OF HEALTH AND HUMAN SERVICES

3.4 The Committee finds that the majority of recommendations made by the Auditor-General following the performance review of fraud control within the DHHS have been implemented.

3.5 With regard to the implementation of recommendation 9 the DHHS has revised the standard Statement of Duties to reflect the DHHS's positon with regard to fraud. Each Officer's obligation and responsibility in relation to the management of fraud is reflected within the standard Statement of Duties. The full implementation of the recommendation is outstanding until the review of all Statements of Duties to reflect this revision is complete.

3.6 The Committee notes the DHHS's initial slow response toward commencing implementation of the Auditor General's recommendations. The DHHS claimed significant disruption occurring as a consequence of structural changes over this period contributed to the delay.

TASMANIAN FIRE SERVICE

3.7 The Committee finds that a number of recommendations made by the Auditor-General following the performance review of fraud control within the TFS have not been implemented.

3.8 The Committee notes that the transfer of corporate service functions within the TFS to the DPEM provides the opportunity to strengthen its fraud control environment.

3.9 The TFS has indicated that the implementation of Recommendations 1 and 3 are underway. The DPEM has engaged Wise, Lord and Ferguson to undertake an Agency-wide risk review including financial risk and fraud.

3.10 The Committee finds that the process whereby the Auditor-General's Report is received and acted upon by the TFS is not sufficient as no indication was given as to the means of ensuring the recommendations had been assessed and acted upon prior to transfer of corporate functions to the DPEM.

3.11 The TFS response to recommendation 6 at the time of the Auditor-General's Report was that it considers that its size limits the resources available to appoint a Fraud Control Officer, and that these functions are included in the duties of the Director Corporate Services and Manager Finance. The Committee does not accept that this mitigates the risk as the responsibilities of these positions are such that they clearly require oversight from a fraud control perspective. The DPEM has provided assurance that the role of Fraud Control Officer will be considered as part of the Agency wide risk review.

3.12 The TFS has failed to act on recommendation 9.

3.13 The TFS has failed to implement recommendation 13.

3.14 A commitment was subsequently made to implement all recommendations including the development of a Fraud Control Plan by the end of the 2015 calendar year.

SERVICE TASMANIA

3.15 The Committee finds that the majority of recommendations made by the Auditor-General following the performance review of fraud control within the DPIPWE have been implemented.

3.16 Recommendation 9 remains outstanding. The DPIPWE has responded that *"it was not considered feasible for HR to update the individual statements of duties for every senior manager"*[4]. The Committee notes that the agency has a comprehensive Fraud & Corruption Control Policy (FCCP). The DPIPWE claims that the responsibilities of senior managers under the FCCP are made clear through the annual performance management review process. The DPIPWE further claims that these mechanisms address the objectives of this recommendation.

3.17 The Committee recognises the timely progress made by the DPIPWE in response to the Auditor-General's recommendations.

UNIVERSITY OF TASMANIA

3.18 The Committee finds that the majority of the recommendations made by the Auditor-General following the performance review of fraud control within the UTAS have been implemented.

3.19 The Committee notes the timely progress of the UTAS toward implementing the recommendations of the Auditor-General.

3.20 With regard to recommendation 2 the Committee notes that UTAS has not specifically implemented a code of conduct that defines expected behaviour for all employees. The Committee is satisfied that UTAS Control of Fraud and Corruption Policy, which contains a number of elements that establish UTAS's expectation in respect of employee behaviour, addresses the objectives of this recommendation.

[4] DPIPWE Questionnaire, Appendix 1, p. 62

3.21 With regard to recommendation 9 UTAS indicated that senior management contracts remain standard across the organisation and do not specifically reference any one particular policy. The Committee notes that contracts do reference all policies, procedures, behaviour requirements and expectations of senior managers. UTAS claims that senior managers are made aware of and alerted to issues of potential fraud, and managing and controlling those instances of fraud.

GENERAL COMMENTS

3.22 The Committee notes the lack of timeliness by the TFS, the DoE and the DHHS in the implementation of some of the Auditor-General's recommendations.

3.23 It is important that entities undertake to introduce a formal mechanism to ensure the timely review and implementation of the Auditor-General's recommendations.

3.24 The Committee is committed to following up the implementation of the recommendations of this Report within 12 months

4 RECOMMENDATIONS

4.1 Based upon its findings from the follow-up review of the Auditor-General's Special Report 95: *Fraud Control*, the Committee recommends that:

1. All entities introduce a formal mechanism to ensure the future timely review and implementation of the Auditor General's recommendations;

Department of Health and Human Services (DHHS)

2. The DHHS fully implements recommendation 9 to ensure that senior managers' statements of duties include fraud management as a required responsibility;

Tasmanian Fire Service (TFS)

3. The Department of Police and Emergency Management (DPEM) ensures that the TFS fully implements outstanding recommendations, as detailed in Table 4; and

Service Tasmania

4. The Department of Primary Industries, Parks, Water and Environment ensure Service Tasmania implements recommendation 9 to ensure that senior managers' statements of duties include fraud management as a required responsibility.

Hon Ivan Dean

Chair

28 October 2015

PUBLIC ACCOUNTS COMMITTEE

QUESTIONNAIRE

Review of Actions taken in response to Auditor-General's Special Report No.95 *Fraud Control*

OVERVIEW

The Auditor-General's "performance audit was conducted in the context that the incidence of fraud is increasing in Australia".

The State entities included for the purposes of the performance audit were:

- Department of Education;
- Department of Health and Human Services (specifically Housing Tasmania. Ambulance Tasmania and Launceston General Hospital);
- Department of Primary Industries, Parks, Water and Environment (specifically Service Tasmania);
- Tasmania Fire Service; and
- University of Tasmania.

Audit objective:

The audit objective was to assess the effectiveness of fraud management strategies in selected State entities.

Audit Scope:

The audit scope was concerned with:

- Development and implementation of fraud control strategies
- Relevant preventative and detective controls for procurement, accounts management, cash handling, corporate credit cards, payroll and IT systems
- Controls, strategies and policies
- The period from July 2009 to October 2010.

Audit criteria:

The audit criteria developed were aimed at addressing effectiveness aspects including:

- Does a suitable fraud management strategy exist?
- Do internal controls prevent and detect fraud?

Auditor-General's conclusion:

"it is my conclusion that attention needs to be paid, in varying degrees, to the organisational culture at all five entities to improve the effectiveness of the fraud prevention and detection mechanisms currently in place."

DEPARTMENT OF EDUCATION

Audit criteria 1: Does a suitable management strategy exist?

In assessing the effectiveness of fraud management strategies the Auditor-General paid particular attention to the comprehensiveness of Fraud Control Plans and staff awareness of fraud and fraud control.

The findings for the Department of Education are shown in *Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?*

Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?

Fraud control planning	
Definition of fraud and statement of attitud	✓
Code of Conduct	✓
Fraud control planning and review	×
Fraud Control Officer appointed	✓
Internal audit activity	✓
Fraud prevention and detection	
Fraud awareness	×
Management accountability	×
Fraud risk assessment	✓
Personnel rotation and leave management	✓
Employment screening	×
Mechanisms for reporting suspected fraud	✓

✓ Satisfactory level of compliance

× Recommendations made

Audit criteria 2: Do internal controls prevent and detect fraud?

The Auditor-General also examined the design of the internal control framework and internal compliance with the controls.

The findings for the Department of Education are shown in *Table 2: Findings - Audit Criteria 2 – Do internal controls prevent and detect fraud?*

Table 2: Findings – Audit criteria 2 – Do internal controls prevent and detect fraud?

Findings - adequacy of internal controls	
Cash	✓✓✓
Corporate Card	✓
IT	✓✓
Expenditure and procurement	✓
Payroll	✓✓
Receipts and receivables	✓✓

✓✓✓ Internal Controls were well designed and compliance was satisfactory

✓✓ Internal controls were well designed but compliance needs minor improvement

✓ Either internal control design needs improvement or compliance needs major improvement

× Control design needs major improvement

In accordance with *Audit Act 2008* section 30 the Department was provided a copy of the Report by the Auditor-General, together with a request for comment.

The Department provided the following comments regarding specific recommendations which were included within the Report.

Recommendation #:

#8 – DoE undertakes to increase the general level of fraud awareness amongst its employees through internal communications mechanisms;

#9 – DoE will investigate the feasibility of amending managers' statements of duties to include fraud management;

#11 – DoE will investigate an approach to monitor employees leave balances in high risk positions. However, automatic replacement of staff on leave is not financially feasible;

#12 – All school based positions and a number of non-school positions currently have police checks. DoE will investigate this proposal in relation to other high risk positions;

#14 – DoE has recently communicated to staff the reporting mechanisms available to them and will undertake to continue this practice on a more regular basis;

#15 – DoE has tightened corporate card control processes through the implementation of a termination checklist;

#16 – DoE will investigate the feasibility of developing a security plan and the testing of backups;

#17 – DoE will target improved awareness and compliance with delegated authority and will implement more timely review of exception reports;

#18 – Exception reports are now reviewed and retained. In addition, a termination checklist has been implemented; and

#19 DoE will investigate current revenue reporting framework and consider the best approach to this recommendation.

REPORT RECOMMENDATIONS

The Report made a total of 33 recommendations and the following section of the questionnaire provides each Department the opportunity to demonstrate the actions taken in response to the recommendations of the Auditor-General made for that Department.

Supporting documentation can also be provided as an attachment to your response.

A copy of the Report is attached for the information of the Department.

DEPARTMENTAL RESPONSE TO REPORT RECOMMENDATIONS

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Control Planning – in *Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?* it is clear that the Department was consistent in its demonstration of a satisfactory level of compliance in the area of fraud control planning. Even so, the following general recommendation does apply to the Department.

Recommendation 4

All entities should review and amend their Fraud Control Plans at appropriate intervals, as a minimum, once every two years

Department of Education response to Recommendation 4:

A review of the Department of Education's (DoE) Fraud and Corruption Control Plan (FCCP) commenced in September 2014. The revised FCCP has been submitted to DoE's Risk Management and Audit Committee for its meeting on the 23rd March 2015. Upon endorsement from the Risk Management and Audit Committee:

- the policy will be submitted to the Executive for approval (noting that the Executive form part of the Risk Management and Audit Committee); and

- the policy will be communicated to all staff.

The FCCP includes a timeframe for formal review which will be bi-annually.

UDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST? (CONT.)

Fraud Prevention and Detection – *Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?* summarises the fact that a number of recommendations were made in this area for the Department.

Recommendation 8

All entities should introduce mechanisms to ensure that all employees have a general level of fraud awareness that is appropriate for their level of responsibility.

Department of Education response to Recommendation 8:

DoE has increased the general level of fraud awareness amongst its employees through the following:

- 2012 - Presentation at the School Business Managers annual conference by the Manager, Internal Audit Office regarding fraud risks and their management.

- 2013 – Follow up presentation on fraud at the School Business Managers annual conference by the Manager, Internal Audit Office.

- 2014 – Fraud risk management presentation to DoE's Corporate Services Division senior managers by the Manager, Internal Audit Office.

• The Internal Audit Office has between 2011 and 2014 conducted approximately 70 internal audits per annum. These audits included, amongst other things, a review on a sample basis of control over receipting and banking, purchasing and payment payments, journal adjustments, cash security, budget management and corporate cards.

The objectives of these audits is not just to detect and report on instances or areas of non-compliance but also to promote and foster awareness and continuous improvement in the Department's control processes. To this end, auditors take the opportunity during the course of the audit to discuss with the Principal and the School Business Manager the importance of internal control, using observations made during the course of the audit to illustrate the local and broader consequences of not having effective controls in place.

• As stated in response to Recommendation 9, following consultation with all staff in 2014, Statement of Duties for SES, Principals, Assistant Principals and School Business Managers include responsibility for the management of fraud risks. Statement of Duties for Tasmanian State Service Award Band 8 and 9 classified roles are updated to include these responsibilities upon vacancy advertising.

• There are a range of policies that contribute to the fraud framework with communication of those policies and procedures raising awareness of DoE's attitude to an ethical culture being based on all staff conducting themselves in a manner consistent with the law, State Service Principles and Code of Conduct and DOE policies. For example the following actions have occurred:

- General circular was sent to all staff in July 2011 regarding Code of Conduct standards, highlighting amongst other things, ethical behaviour.

- Presentation to DoE senior managers by the Integrity Commission in July 2013 titled "Ethics Session for Managers".

- Review of staff Intranet in 2014 to ensure easy access for all staff to the DoE's Grievance Resolution Policy and Guidelines.

- Presentation to LINC Tasmania Managers by the Senior Conduct and Investigations Officer in May 2014 regarding Code of Conduct standards and Grievance Resolution process.

- Presentation to Child and Family Centre Mangers by the Senior Conduct and Investigations Officer in September 2014 regarding Code of Conduct standards and Grievance Resolution process.

- A general circular was sent to all staff in October 2014 regarding Code of Conduct standards (including ethical behaviour) and Grievance Resolution Policy and Procedures.

- A general circular was sent to all staff in July 2014 on the new Public Interest Disclosures Policy and Procedures.

As noted against recommendation 4, upon the Executive approving the updated FCCP it will be communicated to all staff.

Recommendation 9

All entities should ensure that senior managers' statement of duties include fraud management as a required responsibility.

Department of Education response to Recommendation 9:

In May 2014, consultation was undertaken with all staff on the inclusion of appropriate wording in Statement of Duties relating to fraud management responsibilities. Following this consultation, the Statement of Duties for all SES, Principals, Assistant Principals and School Business Managers were updated to include the following wording in the "Level of Responsibility/Direction and Support" section:

"In the delivery of the Department's activities, the occupant must ensure that:

- Within the occupant's area of organisational responsibility, appropriate strategies are in place to minimise the risk of fraud; and

- Decisions and actions are made ethically and with integrity, on the basis that such is legal, is right and is reasonable based on an objective standard."

Due to the specialist nature of those roles classified at Band 8 and 9 under the Tasmanian State Service Award, Statement of Duties are updated to include this wording as vacancies are advertised.

Recommendation 11

All entities should develop a policy of personnel rotation and ensure that, while employees are on leave, another employee acts in their place.

Department of Education response to Recommendation 11:

DoE monitors employee leave balances. Annually, advice is provided to Principals and managers of employee's whose balances are approaching the upper limits of their award entitlements to assist them in managing leave for these employees and personnel rotation if required.

Within the HR system the Employee Self Service (ESS) module is available to enable all employees to view and self-manage leave balances. ESS also enables managers and principals to review all leave balances to ensure staff access and proceed on leave as required.

The new data warehouse system, Edi, will also deliver 'alerts' via the HR dashboard to managers and principals for employees within their school or business unit regarding high leave balances.

It is not always financially feasible for DoE to replace staff on leave with another staff member. Backfilling of vacancies resulting from leave is determined on a case-by-case basis and is subject to operational requirements, budgets, the potentially critical nature of the position and the availability of staff. However, when an employee is on leave, their duties are usually distributed to other members of staff as resources permit. This assists in reducing the opportunity for fraud and increases the likelihood of detection.

Recommendation 12

All entities should perform police checks for senior or high risk positions and document background checks from previous employers.

Department of Education response to Recommendation 12:

Under current DoE policy, all employees covered by the Tasmanian State Service Award must obtain a DoE Good Character Check (GCC) prior to commencing employment. The GCC includes a National Criminal History Check. All applicants for school based positions are required to complete a GCC. For teachers, the national police check is supplied to the Teachers Registration Board by Tasmania Police as part of the teacher registration process. This may also include an overseas Record of Convictions check (or its equivalent) from the country in which the person is living or has resided for more than 12 months.

Where a GCC is required, the Statement of Duties reflects this, with the following wording inserted in the *Requirements* section as an essential requirement:

"The Head of the State Service has determined that the person nominated for this positon/office is to satisfy a pre-employment check before taking up the appointment, promotion or transfer".

DoE's *Selection Process Guidelines* recommends that selection panels consider a range of verification processes that includes seeking referee reports and contacting people other than cited referees. The GCC process supports this by seeking written permission from the applicant "for the Department of Education to check (my) previous volunteer or employment history, if deemed necessary".

Recommendation 14

All entities should communicate their formalised reporting mechanisms to staff more effectively.

Department of Education response to Recommendation 14:

As noted against Recommendation 8, there are a range of policies that contribute to the fraud framework with communication of those policies and procedures raising awareness of reporting. For example, actions have included

- A general circular was sent to all staff in July 2011 regarding Code of Conduct standards, highlighting amongst other things, ethical behaviour.

- Presentation to DoE senior managers by the Integrity Commission in July 2013 titled "Ethics Session for Managers".

- Review of staff Intranet in 2014 to ensure easy access for all staff to the DoE's Grievance Resolution Policy and Guidelines.

- Presentation to LINC Tasmania Managers by the Senior Conduct and Investigations Officer in May 2014 regarding Code of Conduct standards and Grievance Resolution process.

- Presentation to Child and Family Centre Mangers by the Senior Conduct and Investigations Officer in September 2014 regarding Code of Conduct standards and Grievance Resolution process.

- A general circular was sent to all staff in October 2014 regarding Code of Conduct standards (including ethical behaviour) and Grievance Resolution Policy and Procedures.

- A general circular was sent to all staff in July 2014 on the new Public Interest Disclosures Policy and Procedures.

DoE has recently been participating in the Integrity Commission's Speak-up program. This program is currently promoted on the homepage of the DoE's intranet, accessible to all DoE staff. The aim of the program is to help identify and eradicate misconduct (which includes the misuse of resources). Staff are referred to DoE's grievance resolution process, DoE's Conduct and Investigations Unit, the Integrity Commission and the Ombudsman.

Further, on completion of the review of the FCCP, the FCCP will be broadly circulated to promote fraud awareness and to provide details of DoE's fraud reporting mechanisms.

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD?

In *Table 2: Findings – Audit criteria 2 – Do internal controls prevent and detect fraud?* a number of control areas within the Department were identified as in need of improvement and the following recommendations were made in the context of the audit findings.

Recommendation 15

DoE should improve corporate card controls by tightening relevant administrative processes.

Department of Education response to Recommendation 15:

The DoE has implemented an IT system (Spendvision) that has improved the control, monitoring and administration of corporate card expenditure. Corporate card usage can now be centrally monitored to support supervisors and managers in controlling the extent and use of corporate cards.

In relation to the specific observations made in the report, managers now receive independent advice through Spendvision of corporate card transactions that have been allocated to their school or business unit that require approval. Managers can now also independently review corporate cards issued to their school or business unit, assisting in the identification of corporate cards to be cancelled due to staff separations. Also, the cardholder is not required to obtain a replacement card when internally transferred, reducing the risk that a cardholder may be in possession of two active cards.

More broadly, Spendvision supports internal controls through:

• Automated data retrieval from the card provider on a daily basis

• No delay in waiting for the end of the statement period before the cardholder can start coding their purchases.

• All cardholder details, phone numbers, manager workflows and budget centre access is derived directly from Empower setups of employees

• All cost codes are derived directly from Finance One. No incorrect/inactive codes can be entered in Spendvision.

• All disputed transactions are clearly defined by a separate process in Spendvision which is fully reportable

• All 'private' transactions are clearly defined by a separate, reportable process known as Declined transactions in Spendvision which must be work flowed to a manager and must be repaid to the Department, and the receipt number stored against the transaction

• Merchant groups that are considered to be 'entertainment' are flagged automatically by Spendvision and reports can be run by this flag

• Transactional limit and monthly limits are fully viewable to all cardholders within Spendvision direct from Westpac

• Monthly spending tally is fully viewable to all cardholders on a daily basis within Spendvision

• 100% success rate to reconcile electronic data feed to the direct debit on bank statement each month

• No manual data entry/double entry of credit card transactions into Finance One

• Cardholder managers can view and run reports on cardholder transactions as soon as they appear in Spendvision, and do not have to wait for transactions to be 'sent' to them by the cardholder

• Ability to run reports on end of month statement process and supporting documentation available

• Wide range of reports available in Spendvision for use/interrogation of data by both cardholders, managers and internal audit

For processes outside of Spendvision:

• Corporate Online (Westpac Banking Online system) is set up for credit card reporting to review and audit transactional and monthly credit card limits on a regular basis by Finance area

• Terminated Employees appear daily on automated workflow system report to the Credit Card administrator from Empower and is checked on a daily basis

• Terminated Employees fortnightly report is reconciled against Cardholder Master Sheet on a regular basis by the Finance area

• Employee terminations automatically disable logins to all network systems – including Spendvision – to prevent inappropriate access after an employee has left the organisation

• Disputed transactions process is clearly documented on the Department's intranet for end user awareness

• Monthly review and reporting on the number of Declined Transactions across the Department by the Corporate Card Administrator

• Standard fraud detection service is provided by Westpac

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD? (CONT.)

Recommendation 16

DoE should develop and implement:

- an IT security plan that covers all aspects of the IT environment, particularly those aspects that relate to fraud prevention and detection;

- a regular schedule for testing.

Department of Education response to Recommendation 16:

Back-ups/Testing

DoE utilises a policy driven enterprise grade backup software engine that uses Intelligent Data Agents to capture backup data using the most appropriate mechanism for the data type in a Disk To Disk to Tape backup structure.

DoE has all its production servers at the two government data centres (provided by TasNetworks) with the backup environment located offsite at the 75 Campbell St site.

Details of backup retention schedule consist of:

- Daily Backups, retained for 7+ days
- Weekly Backups retained for 4+ weeks
- Monthly Backups retained for 11+ months
- Half yearly Backups (End of Year & End of Financial Year) retained for 4+ years*

*Note: As backups are viewed as a disaster recovery tool not an archival mechanism, backups are not kept indefinitely.

Verification of backups is managed by exception based upon automated thresholds set against backup logs each night. The retention schedule and types of backups do allow for at time restores to take place, but depending upon the system this may involve a large number of steps and time to achieve.

Backups are used on a very regular basis as the basis to enable data refreshes for the Test / Development and Pre-Production server environments when we are undertaking upgrades or changes to business applications.

The DoE backup process and guidance to staff are reviewed on a regular basis. Refer to the document Department of Education Backup Processes and Policies for further details (Attachments 1 and 2)

DoE has always identified the most important business applications to make sure that the IT infrastructure, processes and support for these are as solid and as robust as possible within the allocated resources. This list is known as the Priority One Applications (refer Attachment 3)

DoE has previously had an Information Management Committee which had a focus in addition to records and document management on identifying the key information assets (business systems) and associated risks.

Security

ERM

DoE has an automated Identity Management system ERM which is both position and role based, and provides automatic security settings in most IT systems based upon the base employee data in Empower. If a staff member moves sections or leaves DoE, once the changes are made my HR in Empower then they automatically flow into security settings in IT systems.

ERM performs the following automatic core functions:
- Account Provisioning including role management and group membership/ De-Provisioning of same
- Resource Provisioning / De-Provisioning

ERM is also fed student data from EduPoint via the data warehouse DW3 and handles the automatic provisioning/de-provisioning of most IT resources including Active Directory Accounts, Resources, etc for the student and their classes.

Manual Account Provisioning/Self servicing
ERM is also used for manual provisioning of access to Resources, Systems and Applications allowing management of permission provisioning to be delegated to clients (E.G managers of Organisational Units) through a front end web application (vkey) can enable staff to see file resources that otherwise would be hidden from them.

Staff self-servicing
Staff and students can also use a system called vkey to self-manage their own account allowing them to reset their passwords.

Policy

With the advent of Whole of Government Information Security Policy, DoE established an Information Security Committee to replace the Information Management committee. The Information Security Committee is currently developing an Information Security Plan as required by the Tasmanian Government Information Security Policy Manual. Implementation of the Information Security Plan will assist in mitigating fraud risk by:

- Developing appropriate risk management strategies.
- Direct the preparation, review and approval of the agency's information security policy framework.
- Ensure that the implementation of information security controls is coordinated across the agency.
- Review and approve methodologies and processes for information security.
- Assign responsibility for and oversee the management of information security registers.

Recommendation 17

DoE should:

- tighten controls surrounding payment authorisation;

- ensure that all exception reports produced are properly reviewed and that an appropriate audit trail exists in the expenditure and procurement areas.

Department of Education response to Recommendation 17:

A new financial information and management system, Finance1, was implemented in schools in 2012/13. This is the same system used by the non-school sector of DoE. All payments can now only be made by the electronic authorisation of two, independent people. Who can approve payments is managed by the logical access controls of Finance 1. There is further segregation in the payment process in that although schools and business units have the ability to approve the payment, the finalisation of the payment and transfer of funds to the supplier can only be processed by the DoE's centralised accounts payable staff.

Finance 1 also provides a strong audit trail. It captures details of the payment as well as by whom and when the transaction was entered, approved, posted and paid to the supplier.

In relation to the observation made in the audit report regarding creditor creation exception reports, independent reviews of all creditor creations within Finance 1 are now completed on a weekly basis.

Recommendation 18

DoE should:

- ensure that all exception reports produced are properly reviewed and retained in the payroll area; and

- develop a termination checklist to ensure employees' access privileges are removed.

Department of Education response to Recommendation 18:

DoE has developed a fortnightly certification process to ensure that HR operational staff are checking payroll exception reports that are returned for each pay period by schools or business units. There are automated mechanisms within this certification process to alert senior staff when schools or business units fail to certify fortnightly payroll information. This process enables HR staff to follow up directly with the school or business unit regarding the required certification.

Operational staff within HR follow a termination checklist with employee separations. As part of this process, when an employee separates from DoE this is entered in the HR system whereby access is then automatically removed from close of business on their date of separation. This occurs through an interface to the IT system (ERM) which updates from an overnight load, removing IT permissions from the HR system.

The ERM Identity Management system is both position and role based in automatically providing security settings in most IT systems based upon the base employee data in Empower. If a staff member moves sections or leaves DoE, once the changes are made my HR in Empower then they automatically flow into security settings in IT systems.

(refer Attachments 4 and 5 – HR termination checklists)

Recommendation 19

DoE should compare actual cash receipts to budgeted cash flow in all areas so that variances are promptly identified and investigated appropriately.

Department of Education response to Recommendation 19:

The introduction of Finance 1 across all areas of DoE (school and non-schools) has allowed all business units of the DoE to run ad hoc or periodic reports that can be utilised to monitor actual to budgeted cash flows or against proportionate budgeted cash receipts.

Monthly reports are provided to DoE's executive group detailing the budget performance of school and non-school based business units.

DoE has also released an on-line financial dashboard reporting system (as part of a broader system called E*d*i). The dashboard provides reporting on key aspects of financial management (refer Attachment 6) and school details are viewable by all staff in each school.

PUBLIC ACCOUNTS COMMITTEE

QUESTIONNAIRE

Review of Actions taken in response to Auditor-General's Special Report No.95 *Fraud Control*

OVERVIEW

The Auditor-General's "performance audit was conducted in the context that the incidence of fraud is increasing in Australia".

The State entities included for the purposes of the performance audit were:

- Department of Education;
- Department of Health and Human Services (specifically Housing Tasmania. Ambulance Tasmania and Launceston General Hospital);
- Department of Primary Industries, Parks, Water and Environment (specifically Service Tasmania);
- Tasmania Fire Service; and
- University of Tasmania.

Audit objective:

The audit objective was to assess the effectiveness of fraud management strategies in selected State entities.

Audit Scope:

The audit scope was concerned with:

- Development and implementation of fraud control strategies
- Relevant preventative and detective controls for procurement, accounts management, cash handling, corporate credit cards, payroll and IT systems
- Controls, strategies and policies
- The period from July 2009 to October 2010.

Audit criteria:

The audit criteria developed were aimed at addressing effectiveness aspects including:

- Does a suitable fraud management strategy exist?
- Do internal controls prevent and detect fraud?

Auditor-General's conclusion:

"it is my conclusion that attention needs to be paid, in varying degrees, to the organisational culture at all five entities to improve the effectiveness of the fraud prevention and detection mechanisms currently in place."

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Audit criteria 1: Does a suitable management strategy exist?

In assessing the effectiveness of fraud management strategies the Auditor-General paid particular attention to the comprehensiveness of Fraud Control Plans and staff awareness of fraud and fraud control.

The findings for the Department of Health and Human Services are shown in *Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?*

Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?

Fraud control planning	
Definition of fraud and statement of attitud	✓
Code of Conduct	✓
Fraud control planning and review	✓
Fraud Control Officer appointed	✓
Internal audit activity	✓
Fraud prevention and detection	
Fraud awareness	×
Management accountability	×
Fraud risk assessment	×
Personnel rotation and leave management	×
Employment screening	×
Mechanisms for reporting suspected fraud	✓

✓ Satisfactory level of compliance

× Recommendations made

Audit criteria 2: Do internal controls prevent and detect fraud?

The Auditor-General also examined the design of the internal control framework and internal compliance with the controls.

The findings for the Department of Health and Human Services are shown in *Table 2: Findings - Audit Criteria 2 – Do internal controls prevent and detect fraud?*

Table 2: Findings – Audit criteria 2 – Do internal controls prevent and detect fraud?

Findings - adequacy of internal controls	
Cash	✓✓✓
Corporate Card	✓✓
IT	✓
Expenditure and procurement	✓
Payroll	✓✓
Receipts and receivables	✓✓

✓✓✓ Internal Controls were well designed and compliance was satisfactory

✓✓ Internal controls were well designed but compliance needs minor improvement

✓ Either internal control design needs improvement or compliance needs major improvement

× Control design needs major improvement

In accordance with *Audit Act 2008* section 30 the Department was provided a copy of the Report by the Auditor-General, together with a request for comment.

The Department provided the following comment.

> The Department of Health and Human Services welcomes the Auditor-General's report on Fraud Control and agrees with the recommendations made. The Agency considers its Fraud Control Plan to be comprehensive and will continue to promote awareness to its employees. The Agency, the Launceston General Hospital, Ambulance Tasmania and Housing Tasmania take note of the specific points that are raised and will give consideration to their implementation either across the Agency as a whole or in the areas audited.

REPORT RECOMMENDATIONS

The Report made a total of 33 recommendations and the following section of the questionnaire provides the Department the opportunity to demonstrate the actions taken in response to the recommendations of the Auditor-General. Supporting documentation can also be provided as an attachment to your response.

A copy of the Report is attached for the information of the Department.

DEPARTMENTAL RESPONSE TO REPORT RECOMMENDATIONS

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Control Planning – in *Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?* it is clear that the Department was consistent in its demonstration of a satisfactory level of compliance in the area of fraud control planning. Even so, the following general recommendation does apply to the Department.

Recommendation 4

All entities should review and amend their Fraud Control Plans at appropriate intervals, as a minimum, once every two years

Department of Health and Human Services response to Recommendation 4:

The Fraud Control Policy and Plan were revised in January 2014 and are currently undergoing further revision to incorporate new policies and procedures implemented in July 2014 by DHHS Strategic Control Workforce and Regulation- HR. Revision date for these will be set for 2016.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST? (CONT.)

Fraud Prevention and Detection – *Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?* summarises the fact that a number of recommendations were made in this area for the Department.

Recommendation 8

All entities should introduce mechanisms to ensure that all employees have a general level of fraud awareness that is appropriate for their level of responsibility.

Department of Health and Human Services response to Recommendation 8:

In 2014 Internal Audit completed a series of fraud awareness workshops across the department for all staff at team leader leave and above. An outcome of the workshops was the development of a fraud action plan for each unit that team leaders will discuss with staff members in team meetings.

Also, as part of this process a fraud awareness self-assessment tool was developed in the form of a questionnaire that will be completed every 2 years by each business unit to monitor ongoing awareness within each unit.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST? (CONT.)

Recommendation 9

All entities should ensure that senior managers' statement of duties include fraud management as a required responsibility.

Department of Health and Human Services response to Recommendation 9:

DHHS will implement changes to the wording contained in its Statements of Duties to communicate its position on fraud and to inform workers (including senior managers) of the obligations and responsibilities they have in relation to fraud prevention and management.

The Statement of Duties template will be updated by 31 December 2014 and changes made to current Statements of Duties as they are reviewed from January 2015.

Recommendation 10

Launceston General Hospital, Ambulance Tasmania and Housing Tasmania should evaluate all internal and external risks pertaining to the entity, particularly those relating to fraud, and amend the current risk register accordingly.

Department of Health and Human Services response to Recommendation 10:

The Department of Health and Human Services (DHHS) is implementing a new Enterprise-wide risk management framework in 2014-15. Strategic level risks were assessed and documented against the new framework between February and June 2014.

All DHHS Groups, including Ambulance Tasmania and Disability, Housing and Community Services participated in risk assessment workshops during this period and documented their top risks in strategic risk profiles.

These risk assessment workshops were conducted in addition to fraud prevention workshops, which had a specific focus on the fraud risk assessment tool produced by Internal Audit.

A new DHHS Risk Management Policy was issued on 1 July 2014 and the new framework is being rolled out across business units over the remainder of the 2014-15 financial year.

Under the roll-out plan, all DHHS business units are required to review and/or assess their risks against the new framework by the end of December 2014, and document their risk registers by February 2015. Risk treatment plans are to be developed, approved, reported and, where required, escalated in accordance with the new framework between March and May 2015.

The Launceston General Hospital (LGH) as a part of the Tasmanian Health Organisation – North (THO-N) has evaluated the risks pertaining to the entity and has a comprehensive integrated management risk policy.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST? (CONT.)

There are also a number of committees in place within THO-N to govern risk management. These include the Governing Council Audit & Risk Subcommittee, Integrated Risk and Quality Committee and the Quality, Safety and Clinical Risk Subcommittee. These subcommittees convene on a monthly basis.

The evaluation of the organisations fraud exposure has been undertaken from a variety of internal and external audit reports undertaken since 2011 where no issues of fraud have been raised with management.

Recommendation 11

All entities should develop a policy of personnel rotation and ensure that, while employees are on leave, another employee acts in their place.

Department of Health and Human Services response to Recommendation 11:

DHHS is supportive of the higher level concept that this recommendation is based on (avoiding sole person dependency). The DHHS is unable to commit to the specific and 'no exceptions' nature of the recommendation as currently worded as it is impracticable to implement. While in many cases employees act in another position when an employee is on leave, this is not always the case. In many situations all or some of the duties performed by a worker taking leave are allocated to another worker (or multiple workers) with that worker remaining in their current role. In addition, duties are regularly not performed when the occupant is on leave following the determination that the duties not being performed during the period will have a minimal impact on the achievement of business objectives/service delivery. The requirement to backfill every position when the occupant is on leave would have a significant impact on the DHHS, particularly in the current environment of budget pressures. This requirement would result in increased direct and indirect staffing costs.

DHHS has a *Leave Management Procedure* in place which requires managers to consider a broad range of factors when approving leave requests, including the need to consider if the duties need to be performed during the leave period and, if so, how the duties will be performed. The *Leave Management Procedure* also requires leave entitlement balances to be monitored and not exceed tolerable levels.

DHHS understands the risk that sole person dependency presents in relation to fraud and acknowledges that more work needs to be done to ensure this risk is adequately addressed. The DHHS will explore alternative strategies for addressing this risk.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST? (CONT.)

Recommendation 12

All entities should perform police checks for senior or high risk positions and document background checks from previous employers.

Department of Health and Human Services response to Recommendation 12:

DHHS has a robust *Conviction Check Procedure* in place which requires officers and employees entering the DHHS or moving to another position within the DHHS (regardless of the position's seniority or risk profile) undergo a conviction check prior to commencement, unless exceptional circumstances apply. Conviction checks must also be undertaken for labour hire workers (such as temporary nursing and administrative staff) and volunteers prior to their commencement and may be performed for independent contractors upon the relevant unit's request.

The conviction check process considers an individual's conviction history and the duties they are required to perform in order to make a determination regarding the appropriateness of the individual undertaking the role. The DHHS' position on conviction checks and its supporting processes have proven beneficial for managing fraud related risks.

Reference checks involving contact with previous employers are commonly conducted as part of the selection of employees. Reference checks are not mandatory as it is recognised that in many cases the information obtained from previous employers is subjective and, therefore, holds limited value.

Recommendation 14

All entities should communicate their formalised reporting mechanisms to staff more effectively.

Department of Health and Human Services response to Recommendation 14:

The DHHS Fraud Control Policy and Plan provides formalised reporting mechanisms for fraud related events. The Public Interest Disclosure (Whistle-blower) (PID) Procedure that was implemented in July 2014 also provides formal reporting mechanisms for confidential disclosure t the Secretary of DHHS or the Deputy Secretary Strategic Control Workforce and Regulation, or externally to the Integrity Commission or Ombudsman. It also provides a form that can assist in making a public interest disclosure.

The fraud policy and plan, PID procedure and reporting pathways were communicated during the fraud awareness workshops conducted by Internal Audit in 2014. These documents had also been communicated out from the Secretary as a communiqué to all staff earlier in 2014.

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD?

In *Table 2: Findings – Audit criteria 2 – Do internal controls prevent and detect fraud?* a number of control areas within the Department were identified as in need of improvement and the following recommendations were made.

Recommendation 20

DHHS should improve:

-corporate card controls by tightening relevant administrative processes, particularly in relation to employee location records and cancellation of corporate cards belonging to former employees; and

- compliance with the reconciliation and authorisation controls in the corporate card area.

Department of Health and Human Services response to Recommendation 20:

Employee location records are kept both within Finance One and/or saved electronically to a central drive. The records kept in Finance One record hierarchy reporting, monthly and transactional limits and the correct costing for expenditure. Any paperwork forwarded to DHHS employees which involve corporate cards (ie new applications, confirmation of receiving new cards etc) are scanned and saved to the central drive.

Each fortnight Finance Operations receive a listing of all staff that have left the Department within the last payroll period. This is reviewed by the Corporate Card Administrator and any staff members found to have a card are contacted and the bank is notified immediately and the card is cancelled. The card is also changed to inactive in Finance One at this time.

Corporate card reconciliations are performed monthly upon receipt of the credit card statements. All corporate card reconciliations are authorised by relevant delegates – the delegation matrix is located within the DHHS central directory and is able to be accessed by all staff.

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD? (CONT.)

Recommendation 21

DHHS should:

- develop an IT security plan and password policy that covers all aspects of the IT environment, particularly those aspects that relate to fraud prevention and detection;

- ensure that, where appropriate, computers automatically time-out;

- develop a regular schedule for testing backups;

- improve controls to ensure that access accounts belong to current employees and reflect current roles at Housing Tasmania and Launceston General Hospital; and

- ensure that employees use a unique user ID and password to access all systems and improve server room access controls at Ambulance Tasmania.

Department of Health and Human Services response to Recommendation 21:

A standard password policy controls network logon password complexity, basic access permissions, and expiry criteria. The use of the DHHS "Active Directory" infrastructure by key and critical systems (e.g. Patient Administration System) as an authentication service provides a consistent framework for authentication and access control. The Finance One system uses an additional internal security mechanism for access to the system

The default workstation configuration on all DHHS computers locks the screen after 10 minutes of inactivity. This can however be varied by OCIO where it would adversely impact business processes.

The "Commvault" backup infrastructure used to protect all DHHS server infrastructure automatically tests backup sets when moving data between storage pools on a regular schedule. Additionally the ability to recover data from backup is tested on a regular basis as (in addition to Disaster Recovery) it is used to recover data lost through human error. The Finance System is backed up every week night. The most recent system recovery process was undertaken on 3 September 2014 and involved the complete recovery of the system to an alternative non-production environment.

Housing Tasmania system support officers (SSOs) perform quarterly or ad hoc checks for duplicates. While the SSOs have access to two accounts (one single admin account and an individual account each), no individual has two or more logon accounts to their name. The administrator password is also changed on a regular basis. Where there is a period of inactivity, the case is further investigated. These situations rarely occur anymore due to the process described below. Our SSOs obtain HR termination reports on a fortnightly basis. This report is then compared against THIS users and relevant users are deactivated in THIS and Centrelink is contacted to deactivate that user's Single Point Enquiry access. Additionally, the SSOs also respond to requests from the Service Centres to deactivate users.

All network logon accounts are issued to staff via formally managed processes. This is predominantly done by the automated creation of accounts based on staff being 'on boarded' by

Human Resources via the Payrolls system, or by forms countersigned by an appropriate manager and actioned via the OCIO IT Service Centre. Where staff cease employment with the Department or THOs their account is automatically disabled. This covers permanent staff, part time staff, and contractors and locums employed by the Department, Service Groups (e.g. Housing Tasmania and Ambulance Tasmania) as well as the three Tasmanian Health Organisations (which includes the Launceston General Hospital).

Wherever possible staff are required to use their personally issued network logon and password to access IT systems. There are some circumstances where this is not practical (e.g. shared ward computers) and business practices require the use of shared logons.

Access to the Ambulance Tasmania Computer Room is controlled by a separate dedicated security system under the direct control of Ambulance Tasmania. Access to this room is only permitted where it has been explicitly authorised by an appropriate Ambulance Tasmania Officer. Access for maintenance works must be booked in advance and authorised by an appropriate Ambulance Tasmania Officer. Access is controlled using individually issued access cards.

Recommendation 22

DHHS should:

- ensure that the lack of documentation in relation to creditor changes prior to April 2010 is investigated;

- improve internal control at Housing Tasmania to ensure that all invoices are authorised;

- ensure that all orders are properly documented at Launceston General Hospital, possibly by completing implementation of the electronic requisition request process; and

- review system processes at Ambulance Tasmania to ensure that initiation and authorisation are independent.

Department of Health and Human Services response to Recommendation 22:

Internal Audit undertook a review on creation and amendment of creditor accounts in 2011. Testing found that for the majority of creditor creations and amendments, appropriate documentation was on file that had been completed by authorised officers and entered into Finance One by approved users. Some entries were found that did not have documentation to back them up. Further investigation indicated that this was due to the request forms attached to emails sent to Finance being saved incorrectly for a number of files. Recommendations were made.

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD? (CONT.)

The recommendation to improve controls within Housing Tasmania re invoice authorisation is sourced from audit sample testing as part of this review. Two invoices from a much larger sample were found to have not been authorised appropriately. Whilst this represents a relatively low error rate, the management of Housing Tasmania recognises the importance of process controls in this area and have sought to strengthen internal controls accordingly. Subsequent financial audits of Housing Tasmania have undertaken similar testing and have not disclosed any identified errors.

The Launceston General Hospital (LGH) as a part of the Tasmanian Health Organisation – North (THO-N) has a process for proper documentation to be generated and retained for all orders which are generated. Given the number of areas undertaking ordering from a variety of systems, electronic ordering for all orders isn't practical.

As an example when undertaking manual orders, the initial request is completed via a blue non-stock requisition form. This form is then approved by a delegated officer and goes to the appropriate area where an electronic request is then completed based on the details that are included in the original request.

The process is controlled with there being a limited number of people with the delegation to approve the original blue non-stock requisition forms and also limited people with the access to raise the resulting electronic requisition requests.

No issues have been raised via internal or external audits since 2011 with regards to the order processes within THO-N.

The recommendation to review system processes at Ambulance Tasmania to ensure that initiation and authorisation are independent relates to the finding that purchase orders raised by an employee could be referred to their spouse (another employee) for authorisation. The controls within Ambulance Tasmania's purchasing system ensure that there is always a separation of duties between the raiser of a purchase order and the approver. Wherever possible, a familial relationship between the employee who raises the purchase order and the approver is avoided. If this situation cannot be avoided to ensure timely operations processes exist for the transaction, approval is reviewed by a third party.

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD? (CONT.)

Recommendation 23

DHHS should ensure that:

- all exception reports produced are properly reviewed and retained in the payroll area; and

- all changes to the payroll database, such as appointments, terminations and changes in pay are reviewed by independent officers in the Pay and Personnel Unit.

Department of Health and Human Services response to Recommendation 23:

All exception reports are produced prior to the finalisation of each pay. These are reviewed by senior members of Payroll Services. These reports are actioned, signed off and filed in current pay order.

All supporting documentation for appointments, terminations etc are forwarded to Payroll Services from Human Resources. Any changes to the payroll database are checked against this supporting documentation and signed off by a senior member of Payroll Services prior to close of pay.

TASMANIA FIRE SERVICE

Response to Fraud Control Audit by Auditor_General, Special Report No. 95

Rec No	Section	Auditor General's recommendations re TFS	TFS Response	Action Officer	Remarks
1	1.2.1	… TFS should: ▪ adopt a fraud definition that aligns with the definition of fraud in either AS 8001-2008 or the Commonwealth Fraud Control Guidelines ▪ develop a statement of attitude to fraud ▪ communicate the fraud definition and statement of attitude to fraud to all employees.	TFS has recently developed and agreed on a set of values. While fraud is not specifically mentioned it is encompassed in these principals. The four values are Service, Professionalism, Integrity and Consideration. Integrity includes being trustworthy and ethical, treating each other fairly and honestly and having the courage to do the right thing. TFS will adopt a fraud definition, develop a statement of attitude to fraud and communicate this to all TFS members.	**DCS**	The TFS has not developed a specific Fraud Control Plan, however has worked closely with internal auditors (Wise, Lord and Ferguson) to understand the potential fraud risks to the organisation. The main areas identified were in respect to financial systems administration and cash receipting within retail areas. The TFS is now implementing the recommendations from these reviews and as part of a broader DEPM environment will adopt a Fraud Control plan.

Rec No	Section	Auditor General's recommendations re TFS	TFS Response	Action Officer	Remarks
3	1.2.3	… TFS should develop comprehensive Fraud Control Plans that address specific fraud risks relevant to them.	TFS is currently implementing a new finance system (Technology One). As a part of this implementation there will be a review of financial controls and risks. TFS will develop a Fraud Control Plan.	**DCS**	This will be completed once risk review is completed (currently in draft form and likely to be completed by June 2015).
4	1.2.3	… TFS should review and amend their Fraud Control Plans at appropriate intervals but, at a minimum, once every two years.	Once developed TFS will review its Fraud Control Plan bi-annually.	**DCS**	Once adopted this will form part of the Department's policy review framework.
6	1.2.4	… TFS should consider assigning the role of Fraud Control Officer to manage their exposure to this risk.	TFS considers its size limits the resources available to have a specialist internal audit role or a fraud control role. These functions are implicitly included in the duties of the Director Corporate Services and Manager Finance, who have the responsibility to review systems and procedures.	**DCS**	Since the time of the Audit the Department has appointed internal auditors (wise, Lord and Ferguson) and now participates on the Department of Police and Emergency Management Audit Committee. As part of a review of DPEM Corporate Services (covering Police, Fire and SES) the role will be considered.
7	1.2.5	… TFS should revise its decision to not have an internal audit function.	TFS considers its size limits the resources available to have a specialist internal audit role or a fraud control role.		

Rec No	Section	Auditor General's recommendations re TFS	TFS Response	Action Officer	Remarks
8	1.3.1	… TFS should introduce mechanisms to ensure that all employees have a general level of fraud awareness that is appropriate for their level of responsibility.	TFS considers that staff have a general level of ethical behaviour and awareness, which is considered to incorporate the same principles as fraud awareness. TFS will include fraud awareness in its induction program (timeframe).	**DHS**	Ethical behaviour and awareness are an important part of Values training.
9	1.3.2	… all entities should ensure that senior managers' statements of duties include fraud management as a required responsibility.	TFS will consider introducing into its senior managers' statement of duties fraud management responsibilities.	**DHS**	This has not been addressed as a priority. However fraud will be addressed in future SODs from (timeframe).
10	1.3.3	… TFS should evaluate all internal and external risks pertaining to the entity, particularly those relating to fraud, and amend the current risk register accordingly.	TFS will review its current risk register particularly in relation to fraud.	**DCS**	The DPEM has engaged WLF to undertake a review of the Departments risk management framework and this will be considered as part of this. As per Recommendation 1 a number of reviews have been undertaken of specific areas of risks and are now being addressed. Progress against these is recorded and reported back to the Audit Committee on an ongoing basis.

Rec No	Section	Auditor General's recommendations re TFS	TFS Response	Action Officer	Remarks
11	1.3.4	… TFS should develop a policy of personnel rotation and ensure that, while employees are on leave, another employee acts in their place.	There have been efforts, particularly in Finance, to cross-train staff in order to allow for personnel rotation. However, the resources available for this are limited, particularly given the size of the organisation.	**MF**	Such a policy is problematic due to the size of the organisation and specific requirements of each roles. However TFS has managed to offer secondments during the past 12 months and provide opportunities for relief arrangements. The TFS has a policy of backfilling during leave periods as a general rule.
12	1.3.5	… TFS should perform police checks for senior or high-risk positions and document prior employer background checks performed.	TFS has introduced police checks for senior or high-risk positions?	**DHS**	The TFS has a policy 3/04 in regard to the use of police / character checks.
13	1.3.6	… TFS should develop an alternative reporting mechanism and communicate this mechanism to staff, via a Fraud Control Plan.	TFS considers there is a clear reporting mechanism for ethical breaches in the organisation and that this has been clearly explained to all staff.	**DHS**	Our original response remains, however this may be strengthened through inclusion in a fraud control plan.
14	1.3.6	… TFS should communicate their formalised reporting mechanisms to staff more effectively.	This has been done in internal courses delivered by Human Services.	**DHS**	DHS to explore further opportunities for this to occur

Rec No	Section	Auditor General's recommendations re TFS	TFS Response	Action Officer	Remarks
27	2.6.2	… TFS should: ▪ ensure that all bank reconciliations are properly reviewed ▪ improve the strength of electronic fund transfer (EFT) controls.	Process have been implemented to provide monthly reporting on major reconciliations. EFT controls are considered reasonable.	**DCS & MF**	MF to report progress monthly to DCS
28	2.6.3	… TFS should ensure: ▪ compliance with the segregation of duty control in the corporate card area ▪ cancellation of corporate cards for terminating employees.	There is a clear procedure for the segregation of duties in relation to corporate credit cards. Card holders prepare monthly statements with invoices/receipts attached and these are approved by the direct cardholder's supervisor. They are also reviewed and payment authorised by the Manager Finance. A list of all card holders is now produced as part of the Finance Manager's report to the Director Corporate Services. This should strengthen the controls around cancelling terminating employees. There is also a staff separation form that is to be completed prior to finalisation of terminating pay. This is to include certification of the return of corporate cards and other TFS property.	**DCS & MF**	MF to report progress monthly to DCS

Rec No	Section	Auditor General's recommendations re TFS	TFS Response	Action Officer	Remarks
29	2.6.4	… TFS should: ▪ develop a password policy that considers current best practice ▪ improve server room access controls ▪ develop a regular schedule to test backups.	Whilst TFS does not consider that its password policy to be deficient it is aware of more stringent approaches by other organisations. As such it reviews its password policy regularly. In relation to server room access controls TFS is not aware of any major issues but will look to record user access in the future. TFS will develop a testing procedure and determine a regular schedule to test backups.	**MIS**	MIS to report progress monthly to DCS
30	2.6.5	… TFS should: ▪ improve internal control compliance in the expenditure and procurement areas ▪ improve the segregation of duties in relation to entry and payment of invoices in the Finance system ▪ update the financial delegation register ▪ ensure that all exception reports produced are properly reviewed and retained in the expenditure and procurement areas.	TFS considers internal control compliance acceptable, and this is reviewed annually in the audit of the State Fire Commission's annual accounts. Limited staff numbers limit the ability to segregate duties fully. The financial delegation register is reviewed regularly. Exception reports are reviewed, the audit found that the reviews weren't evidenced.	**DCS & MF**	MF to report progress monthly to DCS

PUBLIC ACCOUNTS COMMITTEE

QUESTIONNAIRE

Review of Actions taken in response to Auditor-General's Special Report No.95 *Fraud Control*

OVERVIEW

The Auditor-General's "performance audit was conducted in the context that the incidence of fraud is increasing in Australia".

The State entities included for the purposes of the performance audit were:

- Department of Education;
- Department of Health and Human Services (specifically Housing Tasmania. Ambulance Tasmania and Launceston General Hospital);
- Department of Primary Industries, Parks, Water and Environment (specifically *Service* Tasmania);
- Tasmania Fire Service; and
- University of Tasmania.

Audit objective:

The audit objective was to assess the effectiveness of fraud management strategies in selected State entities.

Audit Scope:

The audit scope was concerned with:

- Development and implementation of fraud control strategies
- Relevant preventative and detective controls for procurement, accounts management, cash handling, corporate credit cards, payroll and IT systems
- Controls, strategies and policies
- The period from July 2009 to October 2010.

Audit criteria:

The audit criteria developed were aimed at addressing effectiveness aspects including:

- Does a suitable fraud management strategy exist?
- Do internal controls prevent and detect fraud?

Auditor-General's conclusion:

"it is my conclusion that attention needs to be paid, in varying degrees, to the organisational culture at all five entities to improve the effectiveness of the fraud prevention and detection mechanisms currently in place."

DEPARTMENT OF PRIMARY INDUSTRIES, PARKS, WATER AND ENVIRONMENT (*SERVICE* TASMANIA)

Audit criteria 1: Does a suitable management strategy exist?

In assessing the effectiveness of fraud management strategies the Auditor-General paid particular attention to the comprehensiveness of Fraud Control Plans and staff awareness of fraud and fraud control.

The findings for the Department of Primary Industries, Parks, Water and Environment (*Service* Tasmania) are shown in *Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?*

Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?

Fraud control planning	
Definition of fraud and statement of attitud	×
Code of Conduct	✓
Fraud control planning and review	×
Fraud Control Officer appointed	×
Internal audit activity	✓
Fraud prevention and detection	
Fraud awareness	×
Management accountability	×
Fraud risk assessment	×
Personnel rotation and leave management	×
Employment screening	×
Mechanisms for reporting suspected fraud	✓

✓ Satisfactory level of compliance

× Recommendations made

Audit criteria 2: Do internal controls prevent and detect fraud?

The Auditor-General also examined the design of the internal control framework and internal compliance with the controls.

The findings for the Department of Primary Industries, Parks, Water and Environment (*Service* Tasmania) are shown in *Table 2: Findings - Audit Criteria 2 – Do internal controls prevent and detect fraud?*

Table 2: Findings – Audit criteria 2 – Do internal controls prevent and detect fraud?

Findings - adequacy of internal controls	
Cash	✓✓✓
Corporate Card	✓✓✓
IT	✓
Expenditure and procurement	✓✓
Payroll	✓✓✓
Receipts and receivables	✓✓✓

✓✓✓ Internal Controls were well designed and compliance was satisfactory

✓✓ Internal controls were well designed but compliance needs minor improvement

✓ Either internal control design needs improvement or compliance needs major improvement

× Control design needs major improvement

In accordance with *Audit Act 2008* section 30 the Department was provided a copy of the Report by the Auditor-General, together with a request for comment.

The Department provided the following comments regarding specific recommendations, and these comments were included within the Report.

Firstly Management notes that the report identified that *Service* Tasmania has paid considerable attention to fraud control with generally well designed internal controls in place and high levels of compliance within the control environment. The report has also identified a number of areas in which improvement can be made to strengthen the fraud planning framework and culture.

The Department will prepare a project plan to specifically respond to the findings in the report. This will address developing a fraud control policy, a statement of attitude to fraud and assigning the role of fraud control to a position within the Department. The project plan will be monitored by the Department's Audit Committee. Part of this process will be to review policies in place at other Government Departments. It should be noted that the Department already has in place a number of elements which will be reflected in the fraud control policy eg. Code of Conduct requirements, *Public Interest Disclosure Act 2002* and related Departmental procedures.

In relation to the specific DPIPWE and *Service* Tasmania findings:

Recommendation 25 – as part of the Department's employee termination checklist, Human Resources informs the Information Services Branch upon termination of the employee in a timely manner and Network Access is disabled. *Service* Tasmania also disables access to STARS on the employee's last day.

A new password policy was developed and implemented in November 2010 which increases password security by enforcing the use of stronger passwords and requirement for them to be changed every 90 days.

Recommendation 26 – new procedures have been implemented to ensure there is evidence of the review of the budget variances that are regularly investigated. This includes recording any reasons for budget variances to ensure there is an appropriate audit trail.

REPORT RECOMMENDATIONS

The Report made a total of 33 recommendations and the following section of the questionnaire provides each Department the opportunity to demonstrate the actions taken in response to the recommendations of the Auditor-General made for that Department.

Supporting documentation can also be provided as an attachment to your response.

A copy of the Report is attached for the information of the Department.

DEPARTMENTAL RESPONSE TO REPORT RECOMMENDATIONS

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Control Planning – in *Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?* A number of recommendations applicable to the Department were made for this criteria.

Recommendation 1

Service Tasmania should:

- adopt a fraud definition that aligns with the definition of fraud in either AS 8001-2008 or the Commonwealth Fraud Control Guidelines;

- develop a statement of attitude to fraud; and

- communicate the fraud definition and statement of attitude to fraud to all employees.

Department of Primary Industries, Parks, Water and Environment (*Service* Tasmania) response to Recommendation 1:

Recommendation 1.1 – Service Tasmania has adopted the definition of *fraud & corruption* as detailed in the attached DPIPWE 'Fraud & Corruption Control Policy (FCCP)' May 2012, section 4 page 4. This definition of fraud aligns with AS8001-2008.

Recommendation 1.2 – Service Tasmania, as a Branch within DPIPWE, has adopted a zero tolerance attitude to fraud as defined in section 6, page 5 of the current FCCP.

Recommendation 1.3 – the definition of fraud and statement of attitude towards fraud was communicated to all employees when the FCCP policy was released in May 2012. It is also communicated during induction training sessions for any new employee, as well as being discussed annually as part of an employee's Performance Management Review (PMR). Section 8(b) of the FCCP, lists how DPIPWE ensures the message is communicated to staff.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Control Planning (cont.)

Recommendation 3

Service Tasmania should develop comprehensive Fraud Control Plans that address specific fraud risks relevant to it.

Department of Primary Industries, Parks, Water and Environment (*Service* Tasmania) response to Recommendation 3:

With assistance from its internal auditor, KPMG, DPIPWE has developed a fraud risk assessment matrix and individual Fraud Risk Management Plans for each Division of the Department. A separate Fraud Risk Management Plan was developed to address *Service* Tasmania's fraud-related risks and the controls in place to mitigate those risks.

In addition to a Fraud Risk Management Plan, *Service* Tasmania has well documented cash handling procedures that are communicated to staff through its Procedural Information Management System. These procedures are subject to regular audit through DPIPWE's annual program of cash handling audits.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Control Planning (cont.)

Recommendation 4

All entities should review and amend their Fraud Control Plans at appropriate intervals, as a minimum, once every two years

Department of Primary Industries, Parks, Water and Environment (*Service* Tasmania) response to Recommendation 4:

DPIPWE's Divisional Fraud Risk Management Plans were finalised in November 2014 incorporating suggestions from the Department's Audit Committee. The Plans will be reviewed within the recommended two year timeframe.

The FCCP will be reviewed every two years to ensure the policy remains up-to-date and relevant. A review conducted by DPIPWE's Finance Branch in 2014 did not recommend any changes to the policy.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Control Planning (cont.)

Recommendation 6

Service Tasmania should consider assigning the role of Fraud Control Officer to manage their exposure to this risk.

Department of Primary Industries, Parks, Water and Environment (*Service* Tasmania) response to Recommendation 6:

The FCCP designates each Division Head as the relevant Fraud Control and Corruption Officer (FCCO) for his or her Division. The FCCO has primary responsibility for overseeing implementation of the FCCP and managing the risk of fraud and corruption in the Division. The FCCO is the initial contact person for reporting any incidents or allegations of fraud or corruption within the Division, and is required to notify the Manager Human Resources, Manager Finance and Secretary within 24 hours of receiving a report.

For *Service* Tasmania, the FCCO is the General Manager, Information and Land Services.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Prevention and Detection – *Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?* summarises the fact that a number of recommendations were made in this area for the Department.

Recommendation 8

All entities should introduce mechanisms to ensure that all employees have a general level of fraud awareness that is appropriate for their level of responsibility.

Department of Primary Industries, Parks, Water and Environment (*Service* Tasmania) response to Recommendation 8:

The FCCP outlines the mechanisms that DPIPWE uses to ensure employees are aware of the policy and the risk of fraud and corruption.

All new employees of DPIPWE (including *Service* Tasmania) are briefed on fraud and corruption during the induction stage. The issue is then reiterated during Performance Management Reviews (PMRs), which occur annually.

The FCCP and other fraud information is available to all employees via the DPIPWE intranet.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Prevention and Detection (cont.)

Recommendation 9

All entities should ensure that senior managers' statement of duties include fraud management as a required responsibility.

Department of Primary Industries, Parks, Water and Environment (*Service* Tasmania) response to Recommendation 9:

It was not considered feasible for Human Resources to update the individual statement of duties for every senior manager. Instead, the FCCP specifies the responsibilities of DPIPWE's senior managers, including senior manager positions within *Service* Tasmania, in relation to fraud and corruption, and they are made aware of these responsibilities annually through their PMR.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Prevention and Detection (cont.)

Recommendation 10

Service Tasmania should evaluate all internal and external risks pertaining to the entity, particularly those relating to fraud, and amend the current risk register accordingly.

Department of Primary Industries, Parks, Water and Environment (*Service* Tasmania) response to Recommendation 10:

DPIPWE's strategic risk profile was recently updated by the Department's internal auditor in consultation with the Department's Executive and approved by the Audit Committee. As noted in the response to Recommendation 3, the Department has also prepared a fraud risk assessment matrix and a set of Divisional Fraud Risk Management Plans. A specific Fraud Risk Management Plan was also developed for *Service* Tasmania.

DPIPWE's Internal Audit Program includes regular, unannounced audits of the Department's cash handling controls at sites independently selected by the Department's internal auditor. The two most recent cash handling audits of *Service* Tasmania premises completed in August 2013 and April 2014 resulted in only two 'Low' rated findings. The findings and agreed Management actions from these and other cash handling audits are systematically followed up by the Audit Committee and are being used to improve internal controls in specific divisions and across the Department.

In addition to cash handling audits, the Audit Committee commissions regular data mining audits to identify anomalous transactions and other information that might indicate fraudulent activity for further investigation. The Audit Committee uses the results of each data mining audit to refine the scope of future data mining audits in consultation with the Department's internal auditor.

All instances of suspected fraud that warrant investigation are recorded in a fraud register, reported to the Audit Committee and Tasmanian Audit Office, and discussed at the Audit Committee's next quarterly meeting. The quarterly meetings include fraud as a standing agenda item and are typically attended by representatives of the Department's internal auditor, Corporate Services Division and the Tasmanian Audit Office. The Committee's discussions focus on Management's actions in response to the suspected fraud, identifying improvements to internal controls, and any necessary follow up compliance work.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Prevention and Detection (cont.)

Recommendation 11

All entities should develop a policy of personnel rotation and ensure that, while employees are on leave, another employee acts in their place.

Department of Primary Industries, Parks, Water and Environment (*Service* Tasmania) response to Recommendation 11:

Service Tasmania has controls in place to ensure personnel rotation occurs, including regular back filling for staff on leave. Personnel rotation is also one of the generic controls examined through the Department's regular cash handling audits.

DPIPWE's Executive Committee receives regular reports on all employees with excessive leave balances. Where necessary, individual leave plans are developed to reduce the balance to an acceptable level.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Prevention and Detection (cont.)

Recommendation 12

All entities should perform police checks for senior or high risk positions and document background checks from previous employers.

Department of Primary Industries, Parks, Water and Environment (*Service* Tasmania) response to Recommendation 12:

Each DPIPWE Division is responsible for deciding whether to perform police checks for senior or high risk positions.

All high risk positions within Service Tasmania are required to satisfy a pre-employment National Criminal History Police Check before taking up appointment, promotion or transfer. The following are included in the check:

- Crimes involving dishonesty;

- Crimes of violence;

- Sex related offences;

- Serious drug offences; and

- Traffic violations, including criminal or traffic charges (excluding parking infringements)

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Prevention and Detection (cont.)

Recommendation 14

All entities should communicate their formalised reporting mechanisms to staff more effectively.

Department of Primary Industries, Parks, Water and Environment (*Service* Tasmania) response to Recommendation 14:

As mentioned in the responses to recommendations 1.3 and 8, employees are informed of DPIPWE's formal fraud and corruption reporting procedures during staff induction, then annually during the PMR process. The FCCP is also available on the Department's intranet.

Service Tasmania's Procedural Information Management System is used to communicate relevant procedures to staff.

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD?

In *Table 2: Findings – Audit criteria 2 – Do internal controls prevent and detect fraud?* a number of control areas within the Department were identified as in need of improvement and the following recommendations were made in the context of the audit findings.

Recommendation 25

DPIPWE should develop and implement:

- a termination checklist that requires notification of employee separations to IT Services in a timely manner; and

- a password policy that considers current best practice.

Department of Primary Industries, Parks, Water and Environment (*Service* Tasmania) response to Recommendation 25:

As part of the Department's employee termination checklist, Human Resources informs the Information Services Branch upon the termination of the employee in a timely manner and Network Access is disabled. *Service* Tasmania also disables access to its Receipting System, STARS.

A new DPIPWE password policy was implemented in November 2010 to increase password security by enforcing the use of stronger passwords and requiring passwords to be changed every 90 days.

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD? (CONT.)

Recommendation 26

Service Tasmania should ensure that an appropriate audit trail exists to support information provided in monthly budget variance reports.

Department of Primary Industries, Parks, Water and Environment (*Service* Tasmania) response to Recommendation 26:

DPIPWE's Receipting and Cash Collection Policy includes procedures to ensure there is an audit trail of any variance reports, including actions for deficient amounts, a register book to record cash shortages, and procedures for conducting unplanned spot checks. This policy refers to section 10 of the FCCP to ensure staff are aware of the procedures in place for reporting suspected fraud.

OVERVIEW

The Auditor-General's "performance audit was conducted in the context that the incidence of fraud is increasing in Australia".

The State entities included for the purposes of the performance audit were:

- Department of Education;
- Department of Health and Human Services (specifically Housing Tasmania. Ambulance Tasmania and Launceston General Hospital);
- Department of Primary Industries, Parks, Water and Environment (specifically *Service* Tasmania);
- Tasmania Fire Service; and
- University of Tasmania.

Audit objective:

The audit objective was to assess the effectiveness of fraud management strategies in selected State entities.

Audit Scope:

The audit scope was concerned with:

- Development and implementation of fraud control strategies
- Relevant preventative and detective controls for procurement, accounts management, cash handling, corporate credit cards, payroll and IT systems
- Controls, strategies and policies
- The period from July 2009 to October 2010.

Audit criteria:

The audit criteria developed were aimed at addressing effectiveness aspects including:

- Does a suitable fraud management strategy exist?
- Do internal controls prevent and detect fraud?

Auditor-General's conclusion:

"it is my conclusion that attention needs to be paid, in varying degrees, to the organisational culture at all five entities to improve the effectiveness of the fraud prevention and detection mechanisms currently in place."

UNIVERSITY OF TASMANIA

Audit criteria 1: Does a suitable management strategy exist?

In assessing the effectiveness of fraud management strategies the Auditor-General paid particular attention to the comprehensiveness of Fraud Control Plans and staff awareness of fraud and fraud control.

The findings for the University of Tasmania are shown in *Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?*

Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?

Fraud control planning	
Definition of fraud and statement of attitud	✓
Code of Conduct	×
Fraud control planning and review	×
Fraud Control Officer appointed	✓
Internal audit activity	✓
Fraud prevention and detection	
Fraud awareness	×
Management accountability	×
Fraud risk assessment	✓
Personnel rotation and leave management	×
Employment screening	×
Mechanisms for reporting suspected fraud	✓

✓ Satisfactory level of compliance

× Recommendations made

Audit criteria 2: Do internal controls prevent and detect fraud?

The Auditor-General also examined the design of the internal control framework and internal compliance with the controls.

The findings for the University of Tasmania are shown in *Table 2: Findings - Audit Criteria 2 – Do internal controls prevent and detect fraud?*

Table 2: Findings – Audit criteria 2 – Do internal controls prevent and detect fraud?

Findings - adequacy of internal controls	
Cash	✓
Corporate Card	✓✓✓
IT	✓✓
Expenditure and procurement	✓✓
Payroll	✓✓✓
Receipts and receivables	✓✓✓

✓✓✓ Internal Controls were well designed and compliance was satisfactory

✓✓ Internal controls were well designed but compliance needs minor improvement

✓ Either internal control design needs improvement or compliance needs major improvement

× Control design needs major improvement

In accordance with *Audit Act 2008* section 30 the Department was provided a copy of the Report by the Auditor-General, together with a request for comment.

The Department provided the following comments regarding specific recommendations which were included within the Report.

UTAS appreciates the value of the Fraud Control Audit and welcomes the Auditor-General's report in contributing to improvements in fraud control. This report both follows and occurs during a time when UTAS, as part of contemporary management practice, has been:

- pursuing a broader agenda of increased risk awareness;
- strengthening its focus around fraud risk;
- upgrading its financial management system; and
- improving its IT security network.

Consistent with other improvement initiatives in this area, UTAS has either implemented, is already in the process of implementing or will address the key intent behind recommendations from this report.

The UTAS Audit & Risk Committee receives and considers a report on the close of internal audit recommendations and progress with these Fraud Control recommendations will be included.

REPORT RECOMMENDATIONS

The Report made a total of 33 recommendations and the following section of the questionnaire provides each Department the opportunity to demonstrate the actions taken in response to the recommendations of the Auditor-General made for that Department.

Supporting documentation can also be provided as an attachment to your response.

A copy of the Report is attached for the information of the Department.

DEPARTMENTAL RESPONSE TO REPORT RECOMMENDATIONS

University of Tasmania overarching response:

The University effectively fully implemented all but two of the recommendations following receipt of the report. In respect to these two matters it is noted that:

- Implementing contemporary practice Password Control has taken longer than initially envisaged and this continues to be rolled out in stages with the intention that it will be fully effective by the end of 2014.

- Similarly, the matter of appropriate police checks has also taken longer than anticipated, but the policy to address this should be fully effective for 2015.

More broadly, the University is committed to preventing fraud and corruption within both the University itself and its controlled entities. We subscribe to the fundamental values of honesty, integrity, responsibility, trust and trustworthiness, respect and self-respect and fairness and justice. In this regard all members of the University community and its entities are required to adopt, promote and demonstrate ethical behaviour through their work practice.

In particular we would highlight the following key elements of University's fraud control framework:

1. Establishment and clear articulation of the University's fundamental values.
2. The existence and operation of an Audit & Risk Committee which has oversight of risk management, internal audit and external audit activities.
3. The existence of a Control of Fraud and Corruption Policy which clearly articulates expectations in respect to fostering an ethical culture, supporting the existence of a fraud risk register and providing commitment to the principles of whistleblower protection.
4. The existence of a Fraud Control Plan.
5. The existence of a Fraud Reporting and Investigation Procedure.
6. The recent approval of a three year Internal Audit Strategic Plan 2015-2017 which incorporates elements designed to consider the fraud and corruption threat. In particular we would highlight the following planned projects for 2015:
   A. A suite of electronic fraud detection scripts (developed in conjunction with other Universities, a fraud forensic investigation company and a software developer). These fraud related data analytic scripts are run regularly and form part of ongoing internal audit activities. The scripts developed and implemented are in respect to accounts payable, vendor master data and payroll with credit card transactions proposed for similar consideration.
   B. A structured and broad 'Control self-assessment' (CSA) program incorporating independent verification activities across key finance and administration processes
   C. Consideration of processes to address research misconduct within the University.
   D. Consideration of processes to identify and effectively address actual or perceived conflicts of interest.
7. It is also noted that a greater level of resource has also be attributed to the Audit & Risk team during 2014

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Control Planning – in *Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?* it is clear that the Department was consistent in its demonstration of a satisfactory level of compliance in the area of fraud control planning. Even so, the following general recommendation does apply to the Department.

Recommendation 2

UTAS should develop a Code of Conduct that defines expected behaviour for all employees.

University of Tasmania response to Recommendation 1:

While the University does not maintain a formal Code of Conduct, our overarching values require that we lead by example, supporting each other to act with integrity, be accountable, and consistently live our values every day. We subscribe to the fundamental values of honesty, integrity, responsibility, trust and trustworthiness, respect and self-respect and fairness and justice.

The Control of Fraud and Corruption Policy contain a number of elements which establish the University's expectations in respect to behaviour. The policy applies to all members of the University community and to University controlled entities and partnerships. It applies in all dealings whether individually, collectively or corporately.

The Policy includes an ethical environment statement which explicitly addresses:

- The University's stated commitment to preventing fraud and corruption
- The expectation that all members of the University community and its entities adopt, promote and demonstrate ethical behaviour through their work practice
- The University's support to individual staff members to act ethically in all dealings.

On release and periodic update and review, the Policy is subject to a formal process requiring release and solicitation for comment across the University network as part of the review and approval process.

It is also noted that as part of regular periodic meetings that Audit & Risk officers have with all portfolio owners (Faculty Deans & General Managers, Divisional & Institute equivalents) on risk management matters, the fraud threat is considered and highlighted for communication and awareness at respective Executive meetings.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Control Planning (cont.)

Recommendation 4

All entities should review and amend their Fraud Control Plans at appropriate intervals, as a minimum, once every two years

University of Tasmania response to Recommendation 4:

The University's Control of Fraud Policy also incorporates the Fraud Control Plan. This Plan incorporates fraud related guidance on:

- Planning & resourcing
- Prevention
- Detection
- Response

As part of regular periodic meetings that Audit & Risk officers have with all portfolio owners (Faculty Deans & General Managers, Divisional & Institute equivalents) on risk management matters, the fraud threat is considered and highlighted for awareness and communication at respective Executive meetings.

The Control of Fraud Policy, and related Plan, are subject to impending review and update following the recent appointment of the Director, Audit & Risk.

The fraud threat is also subject to consideration in structuring a balanced risk based program of internal audit activities. In particular it is noted that at present the recurrent internal audit program includes:

- On-going data analytic activities initially in respect to accounts payable transactions, vendor master data and payroll data with the intention to extend this to credit card transactions.
- Control self-assessment activities, particularly in respect to key finance and administration processes including accounts payable and payroll.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Control Planning (cont.)

Recommendation 5

UTAS should promptly implement internal audit's recommendations

University of Tasmania response to Recommendation 5:

Immediately prior to the Tasmanian Audit Office project, the University had undertaken an internal audit project considering the fraud threat. The output from this internal audit project was considered by the Audit & Risk Committee in December 2010 and identified nine recommendations. In this regard, the University formally considered each of the recommendations raised in the internal audit report and specifically addressed risk exposure in respect to each.

It is noted that in respect to one recommendation, to strengthen prospective employee screening processes (refer Recommendation 12), a criminal record check policy requirement has been developed for consideration by the University Senior Management Team towards the end of 2014.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST? (CONT.)

Fraud Prevention and Detection – *Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?* summarises the fact that a number of recommendations were made in this area for the Department.

Recommendation 8

All entities should introduce mechanisms to ensure that all employees have a general level of fraud awareness that is appropriate for their level of responsibility.

University of Tasmania response to Recommendation 8:

Subsequent to the internal audit and Tasmanian Audit Office fraud related projects the following activities were undertaken in respect to highlighting fraud awareness across the University:

- Fraud related policy documentation has been circulated to relevant staff.
- A series of emails and face to face follow up meetings were initiated by the Director, Audit & Risk with all portfolio owners, being Faculty Deans & General Managers, or Divisional & Institute equivalents. This included requesting the fraud threat and the University's position in respect to fraud be brought to the attention of the respective portfolio Executives.
- Targeted training sessions for particular at risk staff groups was undertaken. This included the Major Projects Unit.

In addition it is noted that the current Staff Agreement specifically addresses disciplinary implications for staff in respect to serious misconduct which includes instances where staff engage in theft, fraud or assault.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST? (CONT.)

Recommendation 9

All entities should ensure that senior managers' statement of duties include fraud management as a required responsibility.

University of Tasmania response to Recommendation 9:

The approach adopted by the University is that all senior management contracts of employment include requirement to become familiar with and comply with all University policies and procedures. This includes the control of Fraud and Corruption Policy and the Fraud Reporting and investigation Procedure.

It is also noted that all senior management position descriptions include explicit reference to the University's statement of values which subscribe to the fundamental principles of honesty, integrity, responsibility, trust and trustworthiness, respect and self-respect, fairness and justice.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST? (CONT.)

Recommendation 11

All entities should develop a policy of personnel rotation and ensure that, while employees are on leave, another employee acts in their place.

University of Tasmania response to Recommendation 11:

In practice, when an employee is absent or on leave, another employee will act in that role. This is particularly the case in our 'mission critical' roles which carry significant delegated authority.

The specific matter of more structured 'personnel rotation' remains under consideration acknowledging the organisational impacts and the rapidly changing environment in which the University has and continues to operate.

It is also worth highlighting that the fraud threat is considered in structuring internal audit activities and specifically in this regard we note the following key aspects:

- The implementation of a range of data analytic routines has been designed with a fraud focus. To date scripts have been developed and run for accounts payable transactions, vendor master data and payroll. Planning for implementation of credit card scripts is also well advanced. It is envisaged that these activities will be conducted on an on-going basis with results reported to the Audit & Risk Committee.
- The Control Self-Assessment (CSA) process has been broadened at the University and now incorporates key finance related processes. One of the key benefits of this activity is the role it plays in increasing management awareness of central responsibilities for respective roles to enable enhancements to the control environment in a timely manner. It is proposed that CSA will be further broadened to also incorporate key student administration processes.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST? (CONT.)

Recommendation 12

All entities should perform police checks for senior or high risk positions and document background checks from previous employers.

University of Tasmania response to Recommendation 12:

A criminal record check policy has been developed and is proposed for consideration by the University's Senior Management Team towards the end of 2014.

It is noted that reference checks are undertaken for all positions with more detailed checking undertaking for senior management positions.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST? (CONT.)

Recommendation 14

All entities should communicate their formalised reporting mechanisms to staff more effectively.

University of Tasmania response to Recommendation 14:

In addition to the Control of Fraud & Corruption Policy, the University has established a Fraud Reporting and Investigation Procedure. This Procedure applies to all members of the University community and to University controlled entities and partnerships. It applies in all dealings whether individually, collectively or corporately.

The procedure:

- States the obligation that all members of the University community have to report suspected fraud.
- Sets out the necessary reporting lines.
- Details the process to be followed when investigating a report of suspected fraud or corruption and also the necessary action required in the instance where evidence of fraud or corruption is identified.

Subsequent to the 2009 internal audit and Tasmanian Audit Office fraud related project, the following activities were undertaken in respect to highlighting fraud awareness:

- The fraud related policy and procedural documentation was circulated to all relevant staff.
- A series of emails and face to face follow up meetings were initiated by the Director, Audit & Risk with all portfolio owners, being Faculty Deans & General Managers, or Divisional & Institute equivalents. This included requesting the fraud threat and the University's position be brought to the attention of the respective portfolio Executives through periodic communication forums
- Targeted training sessions for particular at risk staff groups was undertaken. This included all Major Projects Unit staff.

It is expected that the fraud threat and mechanisms for reporting will continue to be communicated through relevant forums.

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD?

In *Table 2: Findings – Audit criteria 2 – Do internal controls prevent and detect fraud?* a number of control areas within the Department were identified as in need of improvement and the following recommendations were made in the context of the audit findings.

Recommendation 31

UTAS should improve system design to better assist in the performance of bank reconciliations.

University of Tasmania response to Recommendation 31:

At the time of the Auditor-General's performance audit, the University had just implemented a new finance system. With the benefit of time to resolve operational matters and with external and internal audit activity having further considered key finance systems, the bank reconciliation process has been refined.

In particular, we would note that the University has recently successfully implemented an upgrade to the receipting system. This upgrade has enabled enhancements to the bank reconciliation process by:

- Facilitating a greater level of online receipting and reducing direct bank deposits.
- Increasing the extent to which the receipting and matching processes are automated.
- Introduced additional capture of information to facilitate matching receipts.

We would also note that when the Bank Reconciliation Officer has periods of leave, the activities and functions relevant to the role are assumed by another staff member.

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD? (CONT.)

Recommendation 32

UTAS should:

- develop a password policy that considers current best practice;

- ensure that computers automatically lock when left unattended.

University of Tasmania response to Recommendation 32:

The University has recently committed significant resource and effort to assess, and where necessary, enhance security measures in respect to its information systems. In particular, the following relevant action has been taken:

- A number of internal audit projects to specifically consider logical security of key information systems have been undertaken. This has resulted in significant effort and resource being committed to enhancing IT system security. This program of activity remains on-going.
- The recent update of the ICT Access Control Policy.
- The recent update of the ICT Security Policy which requires that:

- All access to University ICT Services and Facilities must incorporate appropriate authentication controls.
- Authentication should, where possible, be provided using a unique username and password which is assigned to each authorised User. Password details must be kept secret, and account details must not be shared.
- All areas of the University are required to employ the account management processes described in the ICT Access Control Policy to manage user credentials for their full lifecycle.
- Authentication methods must support minimum password standards, as defined in the User Password Procedure. In particular, it is noted that passwords must be strong and are required to be changed every 90 days.

More specifically it is noted that the recent implementation of the User Password Procedure supports the continued confidentiality, integrity and availability of the University's Information and Communications Technology facilities.

In this regard it is noted that the University has recently enhanced security and access by introducing a self-service password reset portal. All Students, Alumni and Staff are required to register to the service, which will bring the University's security policy in line with other leading tertiary and government organisations. The implementation of this requirement has resulted from consideration of better practice. The roll out of this requirement continues.

In respect to computer lock out, the University has implemented user lock out for a number of failed logon attempts and for units left unattended for greater than 15 minutes.

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD? (CONT.)

Recommendation 33

UTAS should review changes to the creditor master file on a regular basis and ensure that an appropriate audit trail exists.

University of Tasmania response to Recommendation 33:

Following the initial performance audit, the process to change the creditor's master file was subject to initial review by the relevant area manager. It is also noted that the creditors' master file is subject to on-going and regular review and recently a more exhaustive review has been undertaken which resulted in the following actions:

- Creditors not used in the previous 24 month period have been deactivated.
- Employees who have departed the organisation have been deactivated in the primary finance system.
- Staff responsible for maintaining the creditor master file been reminded of the vendor naming convention. This will become part of the annual training refresher for these staff.
- Monitoring of roles to ensure that sufficient segregation of duties are maintained in respect to maintaining/changing creditor master file data.

In addition, it is also noted that regular periodic data analytics has been implemented as part of the recurrent program of internal audit activity. These procedures include interrogation of vendor master data and accounts payable transactions with regular reporting of outcomes to the Audit & Risk Committee. To date this activity has identified:

- Creditors whose are ABN's have been cancelled and/or are no longer registered for GST. These have been deactivated.
- The highlight of vendor detail within key finance systems who share the same bank account for more detailed review and investigation.

APPENDIX 2 – HANSARD TRANSCRIPT

THE PARLIAMENTARY STANDING COMMITTEE ON PUBLIC ACCOUNTS MET IN COMMITTEE ROOM 1, PARLIAMENT HOUSE, HOBART ON WEDNESDAY 11 MARCH 2015.

AUDITOR-GENERAL'S REPORT 95 - FRAUD CONTROL

Ms CHRISTINA BLUELL, SENIOR AUDIT CONSULTANT; AND **Mr ROSS SMITH**; GENERAL MANAGER, SHARED SERVICES; DEPARMENT OF HEALTH AND HUMAN SERVICES WERE CALLED, MADE THE STATUTORY DECLARATION AND WERE EXAMINED.

CHAIR (Mr Dean) - I remind you that this is a public hearing. The committee is interested in hearing any evidence relevant to fraud control management within your organisation. If you are concerned about the nature of any evidence you may want to give and wish to give it in camera, please make that request of the committee and the committee will make a determination on that. This meeting is being recorded and will be available publicly. You are under parliamentary privilege whilst you are in this forum but immediately you leave here parliamentary privilege no longer applies. This meeting is a follow-up to the Auditor-General's report.

Ross, is there any general statement you want to make?

Mr SMITH - Over the last 18 months in particular within the department we have taken a much stronger approach to the management of risk in general, including establishing a risk management framework which is filtering all the way down the organisation. That has a very strong focus on risk. We recognise we have a lot of improvement to make in managing risk in general and specifically fraud.

We have also increased our focus in certain areas - for example, last year an internal audit within DHHS ran and coordinated a number of fraud awareness workshops for all staff to ensure that people had an understanding of fraud in its full context. Many people generally think it is just about taking money, but it is a bit broader than that. It is about making sure you are filling in time sheets accurately and correctly. We feel the fraud awareness workshops, which will result in action plans that will have to be done by all major business units is a way in which we can embed right across the organisation an awareness of the need to manage fraud a lot better, and to prevent fraud.

We are also doing a number of things in terms of ensuring that as we are reviewing all our statements of duties that provisions are included that make it quite clear for all employees that they have an obligation to be alert to the obligations around fraud management and awareness. It is fair to say we have a lot to improve upon but we are taking a much more coordinated and comprehensive approach than we might have before.

CHAIR - I think you said you have currently targeted staff at team leader level and above in 2014 for these sessions. What about the other staff within the Department of Health and Human Services? Where do they fit in?

Ms BLUELL - The objective is that the team leaders take it down to their staff level. We have something like 11 000 employees and it was very difficult to cover every employee, so the decision was made to ensure the workshops were covered over a seven-week period at team leader positions and above, and these actions plans are to be taken down to the employee sitting beneath team leader level and discussed at team meetings on a regular basis.

CHAIR - Is that now being done by your team leaders?

Mr SMITH - We are developing these plans; that is the next phase. All areas have to start to be able to develop a plan for their area that takes into account the various things.

Mrs TAYLOR - Is there a time line for that, Ross?

Mr SMITH - We are looking to have those completed by May.

Ms BLUELL - At this point in time, the first stage of the action plans, which were initially developed in the workshops, have finally be completed with responsible officers and time frames on those, and they will then form part of what we do. Every month we do a follow-up of outstanding recommendations on audits. They will form part of that to ensure they are following up on their actions they have identified, and that includes that they are incorporating those at team meetings.

Mrs TAYLOR - So the time line?

Ms BLUELL - In a month's time.

Mrs TAYLOR - They should be completed in May and then they will be applied?

Mr SMITH - Yes.

Mrs TAYLOR - How long do think the whole process is going to take?

Mr SMITH - It is a matter of ensuring that it is an ongoing process. As we renew statements of duties where we have things where we include employees' obligations, et cetera, we started that from January this year. It is probably not feasible to be able to review all those in one hit so we do that as we review the PDAs as positions become vacant.

In terms of the regime, once we have those forward management plans - and I know I can speak for my area - that will formulate a general approach where we are ensuring we are doing things. I have a lot of transactional processing areas under my area where we are looking to increase the level of rotation of staff to a particular role so people do not get fixed in a single role and reducing single person dependencies. That is just good management anyway but it has also been identified as a high-risk area.

All areas will have to have those plans in place and there will be periodic reviews of actions against those plans on an ongoing basis, but I think they filter through to the executive.

CHAIR - In relation to that - and the same issue came up with the Integrity Commission in the workshops they were providing - how do you know all your team leaders, for instance, have been a part of this workshop? Do they sign off on a document to say they have been part of a workshop? How is it identified and recorded if people want to go back and check?

Ms BLUELL - We have a participation list that they sign off on at each workshop.

CHAIR - For new employees coming in, is there any training early in the piece in relation to this?

Mr SMITH - Within the induction processes we have a little bit of room to increase there. These are the things such as employee obligations along with things like workplace health and safety responsibilities that managers should be including in their induction plans for new employees, and their obligations on those types of things as well. The other issue is about the e-learning module which we are running.

Ms BLUELL - Part of the workshop process was a questionnaire of awareness of fraud and we are developing an e-learning, online method of taking those questionnaires to the business units every two years. They self-assess every two years and report to internal audit and we monitor their increased awareness and identify whether they need further workshops or any other training in that way. There is an ongoing process being delivered.

Ms FORREST - How far does that extend down? One of you said earlier that fraud can be incomplete or inaccurate completion of a time sheet, for example? Does this go right down to the base-level employee?

Ms BLUELL - The e-learning tool can be applied to anyone and it would be up to the managers in the units to encourage all their staff to apply it.

Ms FORREST - In view of the comment, if it comes down to completing time sheets properly, for example, is there an expectation it will happen?

Mr SMITH - That all employees will be required to -

Ms FORREST - Required to undertake that module.

Mr SMITH - Yes, that will be part of the ongoing management to make sure we are getting people frequently going through that - every couple of years I think.

Ms BLUELL - Every two years.

Mr SMITH - Every two years is the cycle. In other risk areas like workplace health and safety, all employees had to go through a similar thing and we were able to monitor them. As a manager, in my area with 150 people I used to receive - and I would expect

this to be the same - reports across all the areas on how many people had done those courses recently and how many have not for a long time. It is up to me, and I am held accountable by the executive for any lax areas, to ensure that the staff are going through those particular modules.

Ms FORREST - That would include things like mandatory training, that sort of thing? Is it the same sort of process?

Mr SMITH - I think with the fraud awareness workshop - and Christina will be able to speak on it with more detail than me - from the point of view of raising awareness on a lot of these things, it is as much about people being aware of the risk, because if you are aware of the risk you are more likely to be able to take the steps to not put yourself in a position of risk yourself, or to take steps as well in reporting things that you think are a little bit suspect and need attention.

Ms FORREST - On another point you raised, you talked about the statement of duties being updated on a regular basis. Does the statement of duties include the requirements to undertake these e-learning modules and an understanding of the risk associated with fraud?

Mr SMITH - I think it is intended that there will be a requirement - it outlines the employees' obligations as opposed to a direct task.

Ms COURTNEY - Has the statement of duties template been updated as at 31 December, as has been indicated in the response?

Mr SMITH - Yes, that is my understanding. From 15 January we have a generic template for the statement of duties that has a number of those essential items like workplace health and safety, anti-harassment - all of those kinds of things that go on the statement of duties. The information I have is that the statement of duties now, as it is being revised with the new template, has that information.

Ms FORREST - Can you provide a copy of the template to the committee?

Mr SMITH - Yes.

Ms FORREST - That would be helpful.

Mr SMITH - Can I take that on notice?

CHAIR - Take that on notice, thank you, Ross, and provide it to our secretary if you can. There might be other documents referred to as we go through and we will take note of them. We will write to you to remind you of the documents we are seeking.

Ms COURTNEY - Ross, on that statement of duties it was one of the recommendations from the Attorney-General, why did it take so long for the statement of duties template to be updated?

Mr SMITH - I do not have an answer for that as it is not within my area. We probably have been working through a whole program of things we needed to implement, including

updating the policy and a number of procedures. I guess it is something that is probably considered to be less important than getting, for example, the fraud awareness workshop happening. So in terms of a logistics time frame - and I am only speculating - I would ask what is the most important thing. The most important thing would be to increase awareness of our existing staff and then when you have a list of things like updating statements of duties for people who are about to join our organisation, there would be something there perhaps you would do after these procedures.

Ms COURTNEY - For the current ones that are going to be reviewed as they roll over, how long will that process take until you are feeling comfortable that all the statements of duties encompass this?

Mr SMITH - I don't have a time frame for that. I know that, broadly, if you think that we have within DHHS a turnover of about 10 per cent per annum for externals and probably even greater churned internally within the department in terms of positions as well you would normally expect, on the back of the envelope, it would be a process of a couple of years. Meanwhile, for the current occupants, if we are not reviewing their statements of duties to include that in those, they are also subject to the regime of the fraud awareness as well. It is very much a tool for making sure that we capture people at the front end as they come into our organisation. I would expect that it would be something, particularly as we are going through the consolidation process within the department, too, where we are restructuring, and that often involves reviewing statements of duties as well. I would expect that it would be completed within two years, but I don't have a firm time frame on it.

CHAIR - In your office, who is the responsible senior person?

Mr SMITH - In terms of the statements of duties?

CHAIR - Yes.

Mr SMITH - It would be the responsibility for all managers individually as they renew their statements of duty.

CHAIR - Each manager of each department?

Mr SMITH - Within each section, yes.

CHAIR - Each section has that responsibility to do that.

Mrs TAYLOR - You must have a general HR section? Wouldn't HR just do it?

Ms BLUELL - They do the template for it.

Mr SMITH - Yes, but the statement of duties in terms of the whole broader statement of duties for an employee is the responsibility of an individual manager who goes through HR.

CHAIR - The reason I ask that question is, how could you be assured that they are being done when you are saying that you cannot really give us a time frame for it? If it comes

down to a number of individuals throughout the department, and I can understand having to do these separately, how do you know they are being addressed? How do you know they are going to be done? If there is no time line put on it -

Mr SMITH - Every time a statement of duty is reviewed it has to go through, for example, a place called Job Design within our department. That ensures that statements - every time you change anything. That is a rather lengthy process where they take in a range of things making sure the actual duties they are performing are in keeping with the classification. They also make sure all of the core, essential obligations of the employee are up to date.

For the staff within the organisation we have other mechanisms, and more immediate and thorough mechanisms, for dealing with their awareness. That is through the ongoing e-learning, the ongoing awareness and what have you. If you think about the statements of duties as having more of an effect on people coming to the organisation, if we are making sure that we are updating those as a priority for all new people coming into the organisation, that is probably a reasonable thing.

Mr BACON - You would be satisfied then that existing employees and new employees are covered by both of those mechanisms, I suppose?

Mr SMITH - Yes. For example, for a person who has been in your organisation for, say, five years, to try to make a case that they are not aware of what the department's fraud policy is, that would not be a very good argument because there is a policy that is available on the intranet for all staff. It is not an argument for non-awareness if you are an existing employee.

Mr BACON - Because your team leader would have made you aware?

Mr SMITH - Yes, the team leader and the e-learning module that will be developed.

Ms BLUELL - Also when the policies and procedures are updated and put on the front of the intranet in a banner so that they know that these are updated - conflict of interest or public interest disclosure, all those were updated in July and there was a banner of education on the front of the intranet where everyone logs on.

Mrs TAYLOR - Do you test that in any way? How do you test whether your employees are more aware? Are you getting, for instance, more reports of fraud?

Ms BLUELL - Down the track, once the e-learning tool and the questionnaire is in operation, when the reports come back to us, we will be able to determine how many people have responded to them and how many people have answered them and gauge, according to their answers, their level of awareness. Hopefully, over time, we will see a trend upwards.

Mr SMITH - As an example of a similar regime, six months prior to this process we had a very strong focus on workplace safety with a similar mechanism. That information was used by our workplace health and safety experts to inform the next lot of training, or areas of weakness as well, based on the response we received.

Mrs TAYLOR - We are talking about fraud, though, and this is exactly where fraud can occur. For instance - and I am not saying this happens - if your team leader or manager down the track says, 'Twenty staff have done the awareness training', how do you know that is right? Do you ever test the staff and ask if they have done the awareness training?

Ms BLUELL - The e-learning tool will have a reporting mechanism which will identify all the people who have undertaken the questionnaire and that will be reported to internal audit, so independently of the manager we will know who has attended and undertaken the questionnaire.

Mr SMITH - For example, with workplace health and safety, I could ask, at any stage - and I was accountable - for how many staff of the 115 shared services have done this particular module. I had to have 100 per cent completion rate, and this will be the same. It will be possible for me not to just ask for it, but I will be sent it and asked to respond how many people have been going through this particular e-module.

Mr BACON - So of your 150 staff you will reply that, say, 120 have done it?

Mr SMITH - Yes, that would be the sort of information. I would know who hasn't done it and I would say to the managers, 'Here's the information', and as per our policy ensure that people have completed this particular module. In effect, the e-module has that information available to people as to how they are responding in terms of their various understanding.

Mrs TAYLOR - And you think this is foolproof?

Mr SMITH - The module is not our sole strategy because we also have a very comprehensive internal audit program which looks at risks and focuses strongly on fraud. That is another area we have increased our focus on internally in making sure we are addressing those things. In terms of staff awareness of fraud and prevention and management, we think that is a reasonably good ongoing tool, as well as the various face-to-face workshops that are conducted from time to time.

Ms FORREST - The Auditor-General's Report was done in 2010. Your response to the recommendation that all entities should ensure senior managers start introducing fraud management as a required responsibility was that the DHHS will implement changes to the wording, but your response to our questionnaire which was sent out last year was that the statement of duties template would updated by the end of last year and changes made this year.

The cynic in me would say that it was the request from the Public Accounts Committee to get an update that spurred that department into action because for four years that recommendation wasn't followed up. I know Sarah asked why it took so long but I would like a bit more clarification as to why it has taken so long to address the Auditor-General's recommendation. Was it the fact that further follow-up highlighted the need to take action in this area?

Mr SMITH - I cannot personally answer that as I have only been in the organisation less than two years, but we could take that on notice and get you a response.

CHAIR - It is a vital question that most of us probably wanted to ask. Ruth has put it very succinctly and to the point that it has been a concern of ours that has been previously discussed. If you could take that on notice, Ross?

Mr SMITH - Yes.

Ms FORREST - The other question is, was there any other work done prior to the middle of last year in addressing this issue? It seems to me from your response that it did not start until the end of last year.

Ms BLUELL - The fraud framework has been developed since November 2013. We have been developing this methodology to complete this workshop since November 2013 and update all the policies. It is something that cannot happen overnight. It was a major piece of work. The fraud workshops were completed in August and it is the time frame after that in which the actions plans have been developed. All the policies and procedures were updated and implemented on 1 July. All this was prior to this questionnaire being received by us and was being implemented across a period of time.

Ms FORREST - It would be good to have that more detailed response to the committee on that process.

Mr SMITH - Yes. In the time I have been with the organisation I have noticed that over the last 18 months the department and the senior leadership team has recognised that in terms of risk in general we have a long way to go, and this is a major area of risk. I believe we are now putting in some processes in terms of managing all risk, whether it be workplace health and safety, service risk, fraud or whatever, and it takes a bit of time to be able to get it into place. I cannot speak about before I came into the organisation.

CHAIR - We will detail that question to you in writing amongst the other information we are seeking. We will make that clear to the department.

Ms FORREST - Under recommendation 10, that the LGH, Ambulance Tasmania should evaluate all external risks pertaining to the entity, particularly those relating to fraud, and amend the current risk register accordingly, you have made some comments talking about the LGH because that organisation was identified by the Auditor-General. With the plan to move to one Tasmanian health service on 1 July, what work is being undertaken there? The way I have read this, THO North West and THO South have put better risk assessment processes in places than THO North, when the Auditor-General looked at this. What is happening in that regard as we move toward one?

Mr SMITH - I don't feel particularly confident in responding on behalf of THO North, so you probably need to speak with them in terms of specifics. I feel more confident in terms of DHHS but I don't feel confident in responding on their behalf.

Ms FORREST - Who do we need to talk to, then, to find out what is happening? My question is not so much about THO North because it is not going to exist very soon and we are going to have one Tasmanian health service. I am interested in how this is going to be integrated into the one entity.

Mr SMITH - As the council of the THS is formed, they will probably have, as do the current THOs, an audit and risk committee, which is a subcommittee of the council overseeing all risks, including fraud. As an observation, I would say they have also recognised that they probably need to lift their game significantly over the last year or so in some of these areas, but I would think that ensuring there is good, strong governance and compliance with government requirements and checks and balances and things like that would be a core part of how that organisation is formed.

Ms FORREST - I ask again, who do we need to talk to find out what is happening with the Tasmanian Health Service in terms of this area? The Auditor-General did the review at a time when things were different and now we are moving to a different frame again. We have all identified the need to have a really tight process around this, so are you able to get that information from the people involved in establishing the new framework for the one THS, or do we need to talk to someone else specifically?

Mr SMITH - I can speak to someone and see whether we can get a response to you in terms of what specific steps are being taken to ensure this is implemented within the new THS.

Ms COURTNEY - I have a question in relation to that because looking at the answer here with respect to LGH, it talks about the committees in place and the subcommittees that convene on a monthly basis, but it doesn't seem to reflect the focus of the AG's recommendation looking at risks particularly pertaining to fraud. They might be there, they might just not be illustrated in the answer, but the answer to me doesn't seem to, particularly for LGH, focus on the fraud aspect. It talks about all the other types of fraud but doesn't get to the point of the AG's recommendation. The information may be there, but it is just not illustrated in the answer. The last sentence is particularly confusing:

> The evaluation of the organisation's fraud exposure has been undertaken from a variety of internal/external audit reports since 2011 where no issues of fraud have been raised with management.

It doesn't necessarily mean there is no fraud there just because it hasn't been raised with management, so that is a very concerning sentence to me and I would like to get a bit more clarification on that.

Mr SMITH - They are a different agency but I can speak to them about getting some more clarification.

Ms COURTNEY - Thank you.

CHAIR - You are responsible as the manager within Shared Services. What does that incorporate?

Mr SMITH - We have a service delivery framework with the THOs and Shared Services provides asset management.

CHAIR - This is right across the three THOs as they currently exist?

Mr SMITH - Yes, as a service provider, we cover asset management, payroll services, financial process, central financial processing, general statewide procurement contracts

and business systems. For example, in the finance and HR systems, where we address risks and issues raised by an internal audit or Tas Audit, we implement that right across the whole system.

Mrs TAYLOR - So you implement?

Mr SMITH - In those sorts of things, in terms of running the system within Shared Services.

CHAIR - I am having some difficulty in understanding why you haven't had some control across the three organisations in relation to fraud control and the issues raised by Ruth.

Mr SMITH - In terms of the services we provide to the THOs, we certainly have control in the way they are conducted, but if, for example, someone in a THO makes a decision about authorisation of a particular payment or paying a particular employee, we don't have control over that. We have our own controls to make sure the things we receive are properly authorised and paid correctly in accordance with awards, but in the authorisation of those things, we don't have a management role over them, we have a transaction process over some of those.

CHAIR - I am just trying to take that on and look at that in relation to the Police payroll, which is a similar one. That has a central control in Hobart right across the whole of the organisation.

Mr BACON - That is one organisation, though.

CHAIR - It is one organisation but it has different controls around the state of the commanders and so on, but the central body is responsible for ensuring right throughout the whole organisation that authorisations are done properly, that everything meets the necessary requirements of the department to pay and make good the moneys being claimed and so on. There is a central control over that as well.

Mr SMITH - If they have authorised a payment, provided it is authorised by the right person within the THO, we don't have the capacity to determine whether that has happened correctly or not. Having said that, if we identify something in credit card usage which is outside the guidelines, we send our people in. Finance operations would send something to the relative manager to say, 'This appears to be outside the guidelines and we would encourage you to take action or investigate', but we don't have -

Ms FORREST - Is that within the THOs?

Mr SMITH - Within the THOs. We would draw it to their attention but we don't have a management role over it, in the same way as if you issue a payment from your bank to someone, the bank does the mechanics to transfer the money from your account to someone else's account but the bank is not necessarily responsible for whether or not that is an appropriate payment. You have initiated the payment.

Ms FORREST - They do ring up when there is an odd transaction on your credit card. We have probably all had that happen, when someone has committed fraud with your credit card.

Mr SMITH - Yes, we identify as a service to those managers. We would provide that to them and say, 'This appears to be outside of the guidelines and we would encourage you to look into that', because that is the manager's role. The manager needs to be able to make sure they are taking action to investigate whether or not that payment was correct.

Mrs TAYLOR - A broader question is being raised here and that is why we are looking at this. We are looking at the Auditor-General's reports on fraud control and a number of departments, not just yours, that he had findings and shortcomings and made recommendations on. We hoped the Auditor-General's recommendations would have been taken on board at the time they were made. The reason we are looking at this is because they were not. When the Auditor-General's reports come in with recommendations in DHHS, in this case, who is responsible to see that those recommendations are looked at and acted upon?

Mr SMITH - Ultimately the head of agency, and certainly over the last 18 months I would suggest we have taken a lot of action to be able to address those things because we recognised that perhaps we had not addressed those with the haste they deserved.

Mrs TAYLOR - I feel you have been put in the hot seat and I'm not sure you are the people we ought be talking to. That is my concern.

Mr SMITH - Within DHHS -

CHAIR - It is a concern to all of us. When the Auditor-General released this report in relation to fraud control and it came through to your department, who in your department came to you and said, 'We need to implement all of this', or whether you were accepting it or not?

Mr BACON - Ross wasn't there. Ross has only been there for two years.

Mr SMITH - There was a different CFO and a different secretary, but what I can say is what I am aware of now and we are -

Mrs TAYLOR - You have taken it on board now?

Mr SMITH - Yes, certainly, and in terms of risk more broadly. In my experience over that period we have taken a much stronger approach to addressing risk issues around fraud that have been identified by internal audit. I would argue that perhaps in the past those things sat on a list and were not followed up. I think we are taking a stronger approach to that as well. I can only talk in terms of where the department is now and that is that we had a lot of ground to make up. We have a long way to go, but I am pretty confident given the amount of work that we have to do on our risk plans and be accountable for them and whatever, that we are doing it now.

Mrs TAYLOR - If we wanted to be satisfied that these things have been addressed, we could ask the Auditor-General to go back and look at this, I suppose. When do you think that we could ask the Auditor-General to go back and see that for things where there were crosses, or things that were inadequate, have been addressed? Obviously not yet because you are in the process.

Mr SMITH - Yes, and there are quite a few things that have been. For example, conflict of interest in procurement and recruitment, where all members who are on assessment panels now have to actively declare conflicts of interest or, indeed, in some instances fill in things saying that they don't have a conflict of interest in some particular processes. We have increased and encouraged the use of probity advisers in procurement processes to ensure that we have an independent person overseeing panels.

Mr BACON - As you go through those things, will you make it public that these things have been addressed or not? Do you know what I mean? I suppose Adriana's point and the points that you both made before is that these things are being addressed.

Mr SMITH - Yes.

Mr BACON - But how do we have comfort that they are if it is not made public or there isn't some mechanism to inform the committee or the Auditor-General?

Mr SMITH - In terms of reporting on these things -

Ms BLUELL - In the past, the Auditor-General's reports have never come into internal audit, they go to the Secretary and then they will go maybe to the CFO.

Mrs TAYLOR - That is the point of my question, isn't it? How do we get -

Ms BLUELL - Yes. That is exactly right. I raised this last year with the Secretary.

Mrs TAYLOR - What is the point of having this if it is not -

Ms BLUELL - That's right. One of the things that I had discussed with them was to implement that we are involved in every final report that comes in so that we can monitor it. I think that would be a really good way for us to ensure the implementation.

Mr SMITH - On that one, we do have to be careful of that, too, because I don't think we are going to be successful if we think that an internal audit is going to be the sole way to manage these things. Individual managers and individual employees have to understand that it is all about responsibility, just like for workplace health and safety, and that everyone has a role in prevention and management of these issues.

Mrs TAYLOR - That was one of my earlier questions, how do you know that employees have taken this on board and I hear your answer about you all know who has gone through the process, if you like, or who has done the online tool. I am loath to say this, but I am aware you can easily circumvent that system as well - not necessarily your system because I don't know your system, but there are times when questionnaires can be filled in online that you might not necessarily fill in yourself. We are talking about fraud here so there is the potential, I suppose.

Mr SMITH - That is one strategy and that is an important one, awareness -

Mrs TAYLOR - How do you test whether your employees are aware?

Mr SMITH - The other ones are through the ongoing internal audit programs where they have a continuous audit program around particular risk points, including credit card usage. They use sampling and those sorts of things to identify issues where perhaps, if they are not irregularities per se, they are areas where an internal auditor in their judgment might say, 'This looks a little bit weak, it might need a bit of strengthening up'. Then, if it relates to my area, I have to respond and I have to be able to account to the Secretary, that we've addressed that recommendation or that particular point. In terms of your question about whether employees have - you can probably never, ever know 100 per cent whether that individual has taken something on, but we know that education works on one element and we think by a more rigorous approach to our internal audit program and holding managers accountable for addressing the issues they have raised, we feel like we are closing off avenues and risk points as well.

Mrs TAYLOR - I am not for one minute suggesting that what you are doing is not right, because obviously it is great that you are going through the process. My question is only, at the end how do you know, how do you test or measure the success? Are you expecting you will get less fraud or more fraud identification?

Ms BLUELL - One thing with the e-learning tool is, you have to use your own user name and password to log in and use it. If someone else is doing it for you then you have shared your password, which is inappropriate. It has a level of expectation and hope that they do the right thing. Then the report will identify by yes, no and don't know answers, the level of awareness. Hopefully we will see a trend upwards for more understanding of what the fraud environment may look like and incorporate. It will also identify particular business units maybe, or specific areas it might need more workshops and more training to be delivered from Internal Audit or from their own managers themselves. It is still in process and in progress so that is what we hope to see.

Mr SMITH - Our internal audit program where it looks at some of these things is very much also a measurement tool because not only will they look at systematic risks and things theoretically we should be typing up as well, they look at individual transactions. Whilst that isn't sampling, we use that as a gauge of those things where we might pick up some irregularities.

Ms BLUELL - They cover all the really low-level, basic controls that the higher level managers do not have time to consider.

Mr SMITH - But you have looked at individual payments and things and said, did they look reasonable, did they look like they are properly authorised, did they look they have been made on relevant basis.

CHAIR - Ross, the only person within your organisation who could answer our questions in relation to the Auditor-General's report, where did it go, what happened to it, when was it put into action and so on, would be the Secretary?

Mr SMITH - If you want to know about the past, we can get you a response.

CHAIR - We do but I also want to know why. If it passed down the path, say, to you, to the managers, to implement these processes that the Auditor-General has raised and the department has accepted as being of concern to them, you get a part of it, you do what you

are required to do and you then pass that back to who is your next in command, who you answer to -

Mr SMITH - The Deputy Secretary.

CHAIR - The Deputy Secretary then needs to ensure everything is in place and would go back to the Secretary. We would need to be talking to the Deputy Secretary because I would like to know how much the Deputy Secretary has received at this stage in relation to the Auditor-General's report.

Mr BACON - If we want to know what is going on now, you have talked about what is going on now but on the history, we can only have a written response?

Mr SMITH - I can only talk about what is going on now and in terms of these things. Over the last 18 months in my experience of being there, we have different people in place compared to those who were in place in 2010. In my experience, the department is getting its act together and it is tangibly getting its act together on a number of fronts: awareness, audit program, making sure the managers are accountable for tightening up on things. Where we are going now is good and in terms of any future audits we might have through Internal Audit or Tasmanian Audit Office, we will perform better than how we have performed in the past. We will also internally have a range of monitoring and management mechanisms to make sure all managers are accountable for following up on these processes.

CHAIR - Ross, we only have 10 minutes left. I don't know if any member has a new area they want to go into. We need to stick to times because we have a lot of other witnesses.

Ms COURTNEY - Notwithstanding that things have changed and we have covered that now, I want to look at a few more of the audit recommendations. The first one has to do with the personnel rotation. I understand there are budgetary constraints with these types of issues. Looking at the last paragraph of the answer, it says 'DHHS acknowledges more work needs to be done and is exploring ways to address this'. To me that seems a bit of a motherhood statement for quite a clear recommendation. I understand there are economic reasons but after four years of saying you acknowledge you need to look at this in my mind is not a particularly good answer. Is there more work being done on that, rather than just acknowledging it?

Mr SMITH - If we are talking about backfilling, all areas are resourced to be able to manage the leave side of it, so I don't believe additional resources are required there. If you think about it, for every 100 employees, if you look at this literally, it would mean you would have to add an extra 8 FTEs just to manage holidays when the organisation is already resourced to manage leave. It is part of normal management. In terms of rotation and I think a lot of the management plans from managers, in my particular area we are going to have a much greater emphasis on rotation. We are already implementing strategies where we are moving people around so they are not doing the same thing regularly for a number of years. That is not just because of fraud but because it is good management.

Ms COURTNEY - Will you be directing other managers to do that?

Mr SMITH - Certainly within my area, and I know managers are being actively encouraged to do that across the department.

Ms COURTNEY - You have acknowledged it for your department but DHHS is an enormous beast, so can we ensure that people in other locations are looking at this as an important issue? Can it be part of training?

Mr SMITH - Within DHHS, yes. As we restructure we are building these kinds of things where we are moving people through. I would expect for all areas delivering their local risk management plans that there would be an expectation, where it is applicable, that there would be a level of rotation.

Ms FORREST - What about the Tasmanian Health Organisations and the subsequent THS? DHHS is quite a small section of overall health services now. It has been a bit of an issue in that because there will be more employees there than in DHHS the potential for fraud is much greater. Does that apply equally? You are only responsible for DHHS, as you said.

Mr SMITH - I could ask them to provide a response to that if you would like.

Ms FORREST - Otherwise you only get about one-tenth of the picture.

Ms BLUELL - With the THOs a lot of people are shift workers - nurses and doctors - and it is a different environment to a corporate environment where you can rotate duties.

Ms FORREST - But you still have management staff in all those areas, though.

Mrs RYLAH - Could we go back to where Shared Services identifies a transaction that is questionable? I wasn't clear on the process, apart from raising it with the manager of that section. Is a record kept that there is an issue, the degree of the issue, the outcome and how many times this person had these sorts of queries come up? What is the whole management process around that? It sounded a bit loose from my end.

Mr SMITH - We are not necessarily talking, in my experience, about anything particularly big or consistent, but where some of our people may see something on a credit card return, which is rare, where it appears as though it is not within guidelines, so we do not necessarily make a judgment, our staff would typically send that to the finance director, so the senior person, or in some cases I have sent things to the CEO. That is his or her business to take up, as opposed to mine as a service provider, but I am aware they do take it up.

Mrs RYLAH - How are you aware of that, Ross?

Mr SMITH - I would make informal inquiries as to whether or not the service we are providing them is helpful. They are accountable to their CEOs and through them to their boards, and that is how they would manage those things. I had a general curiosity as to how useful this information is and I was pleasantly surprised to find it seemed to be very useful.

Mrs RYLAH - Christina, what is your role as audit consultant in reviewing those transactions, the frequency, the personnel who have been involved and the outcomes?

Ms BLUELL - We undertake a continuous audit program on a six-monthly basis and look at things such as Tasmanian Government card transactions, payments, debtors - it covers the whole gamut of the basic finance and payroll area. It looks at the authorisations, the ability to

get transactions and all the requirements that sit within the policy procedures that relate to any of these types of transactions. When we identify any exceptions they are reported back to the particular entities, recommendations are made and we require them to provide us a response on what they have done about that particular issue.

Mrs RYLAH - Would you get to know of the queries Ross's people may have found or identified? Would you see any report on that from them?

Ms BLUELL - Not specifically. In this area when they look at their credit cards they have what they call a breach letter that is sent out. This is one item of area testing we are talking about incorporating into future control testing for the cards.

Mrs RYLAH - So you're only talking about incorporating that?

CHAIR - Joan, we need to move on because of time. Do you have enough there?

Mrs RYLAH - I would like to complete that if I could because I can see this is an area where -

CHAIR - Okay, Joan, go for it. Ask the question.

Ms BLUELL - We directly test the transactions at the unit level, so outside of Ross's area we go back to the source. It is not necessary to see the breach letters because we identify if there has been a breach or not ourselves.

Mrs RYLAH - Thank you.

Mrs TAYLOR - How many corporate cards are there within the department, what is the credit limit and what is the instance of invalid purchasing? Do you have those details readily available?

Mr SMITH - I can get you the most up-to-date information.

Ms BLUELL - Generally our testing finds very minimal breaches of it. It might be flowers somebody inadvertently bought for someone.

Mr SMITH - Which is an education issue.

CHAIR - That was going to be a question I was going to ask. Since the Auditor-General released this report and it went to your department, do you have any recording of breaches that may have occurred in this area during that period of time, over the last, say, four-year period? It is a very difficult question but I thought you may know if there were any big breaches?

Ms BLUELL - No, I have been working in internal audit for seven years and all the time we have looked at credit card transactions there have only been very minor issues.

CHAIR - Thank you.

Ms FORREST - On further recommendations - and maybe some of this can be provided later. I note that in the Auditor-General's recommendation 12 they should perform police checks for people in higher risk positions, the document and background checks, there is an exceptional circumstances clause in that in your response. I am just interested what would constitute exceptional circumstances and would you check with previous employees who are not named as referees? Often people put referees down that are not going to reveal a problem and there is the opportunity there to talk to other employees who are not named, but are clearly past employees.

Mr SMITH - I guess that the primary purpose of a referee is not necessarily to be able to determine those sorts of issues and that is why we have a comprehensive approach to the conviction check. If it does arise as well, I would say as someone who has employed and conducted a number of those processes as well, if I receive nominated referees who are not someone's immediate supervisor or next-immediate supervisor on their list and is someone who might have no idea, I normally approach that person and would tell them, 'Look, I really need a reference from your last supervisor or the supervisor before that'. I think most managers would be in that habit. There is no value in getting a referee check from someone who is -

Ms FORREST - I agree. What I am saying is, there are exceptional circumstances provisions here and what do they constitute? Particularly in those circumstances, do you dig a bit deeper?

Mr SMITH - I must admit I am not aware of an example of an exceptional circumstance. I am aware that with our conviction checks even if we have people who have been fixed-term employees, or even permanent employees in some cases as well, within the department for, say, three to five years, when they go for a permanent appointment they still have to have a conviction check.

Ms BLUELL - I think where they are talking about exceptional circumstances often they might need to employ someone in a hurry to fill a position and they may not have had time to get these checks back. The conviction checks can take quite some time to be returned, so they might employ that person but still have the checks done.

Mr SMITH - That would be in operation. Certainly I am not aware in my experience in any of the administrative areas where that would have applied.

Ms FORREST - If you could take it on notice there. If there is any other information that can be provided on that I think it would be helpful because it leaves a gap.

Mr SMITH - Yes, I am fairly confident we don't have a lot of gaps on those things. Even when we recruited someone who has been an employee of Police and Emergency Management for 12 years, there were extensive checks and we still performed the full check on that person before they arrived.

Ms FORREST - There are probably other people you might not think you need to do that but you do need to as well. I am just going on to recommendation 14 which talks about, 'all employees should communicate the formalised reporting mechanisms with staff more effectively.' You talk about the fraud policy and plan, the PID procedure and reporting pathways for communicating directly with fraud awareness workshops and these documents

have been communicated out from the Secretary. Are we able to see copies of those documents? They can be provided later for the committee to see what is actually is included.

CHAIR - Yes, they will take that on notice, Ruth. We have them and they will be tabled, here. Anything further, Ruth?

Ms FORREST - The other recommendation probably has an extensive answer, so I am happy to leave it at this stage.

Ms COURTNEY - I have a couple more questions, but I am conscious of time.

CHAIR - Yes, they need to be quick and short.

Ms COURTNEY - Rather than go through all the questions it is probably an overarching comment for the last questions I have. Often the responses don't actually address the specific recommendation of the AG and so that is something I would like to see going forward and depending on the outcome of today is looking back at the recommendation because that is all my questions from here on. We have a wonderful answer which says what a department is doing, but it doesn't answer the recommendation of the AG. That is all my questions are. I think we will be going over similar things and I am conscious of time so I will not ask them all, but maybe on leaving here and depending on how we follow this up as a committee, that can be looked at - making sure the recommendations, notwithstanding what has happened in the past, are addressed.

Ms BLUELL - It could be the process of how that questionnaire came through. It was coordinated by one person outwards and they just received the responses and sent them on.

Ms COURTNEY - So there are lots of things where there is no answer to the AG's recommendations. The department may well be doing it but it is not clearly reflected one way or the other.

CHAIR - Who put these answers together?

Ms BLUELL - The document was coordinated by someone in Strategic Financial Control. For example, LGH's questions probably came from Sonia Purse, the Finance Director. I did the responses on the internal audits through recommendations. The other ones went back to their areas.

CHAIR - Thank you very much for your attendance here today and the way in which you have answered the questions. There are a number of issues we have on notice and we will write to you fairly quickly to seek that further information. It may well be the committee would require a further attendance or attendance of other personnel from DHHS. That is something the committee will determine as we move forward.

THE WITNESSES WITHDREW.

Ms KATE KENT, ACTING GENERAL MANAGER, CORPORATE SERVICES, AND **Mr ADRIAN PEARCE**, MANAGER FINANCE, DEPARTMENT OF PRIMARY INDUSTRIES, PARKS, WATER AND ENVIRONMENT, WERE CALLED, MADE THE STATUTORY DECLARATION AND WERE EXAMINED.

CHAIR (Mr Dean) - Welcome to you both. This is a public hearing being recorded by Hansard. It is in relation to the evidence we require in relation to fraud control management and comes about because of the Auditor-General's Report a few years ago. We sent out a questionnaire to your department and it has now come back to us so we have a number of questions about that. Parliamentary privilege applies whilst you are in this room but once you leave it no longer applies and you are responsible for what you say. If we reach a stage where you feel you would like to give the committee some evidence in camera, for whatever reason, please ask the committee and we will make a determination on that. You have provided answers to a number of questions but is there anything you would like to say at this stage in addition to that?

Ms KENT - Thank you for the opportunity to be here to provide an update on our response. I am representing the department in my role as the Corporate Services General Manager at the moment. I have been doing that since September but my substantive role is as general manager of information at Land Services, which has Service Tasmania within its remit. It is useful to have some knowledge of how that part of the organisation works. Adrian is the manager of the finance branch in the Corporate Services Division and within that role he acts as the custodian for our audit and corruption control policy.

You know about the department and how diverse it is; it is a large department with over nine divisions and some other entities and has over 1 400 staff. Even with such a large agency, we aim to ensure, as we said in our response to you, that from their induction throughout their day-to-day work all staff are aware of audit and corruption control mechanisms in the agency but really that is part of their responsibility as a public servant. We see fraud as just one component of all our behaviours as a public servant.

The other thing to emphasise was that we aim to ensure all managers are aware of their role in embedding corporate policies, such as the fraud policy and procedure. A recent example is when we had our senior manager's forum at the end of last year, 14 November, the Integrity Commissioner came along and spoke to that because John Whittington, our secretary, takes matters of behaving as a public servant and how you do your duty very seriously. That message was about the leadership role all managers have in the agency to commit to these corporate policies. It was important to emphasise that.

Since the report, which was in 2011, there have been actions going on throughout the year to try to ensure our policies and procedures are updated and embedded further into our system. Another emphasis was around making sure they are well communicated through to our staff. They were the key points I wanted to emphasise.

CHAIR - This report from the Auditor-General was completed and provided in 2011 in relation to this area and there were a number of significant issues he identified within your department. What happened from the time the Attorney-General brought those matters to your attention until now? How long has it taken to get this moving forward and put some of these things into action? What have you done?

Ms KENT - Overall, many of the findings and recommendations he made were emphasising where we needed to improve how we did something that probably existed but either was not well articulated or needed to be clarified. I would not say they were significant suggestions. They were things about improving existing practices and making sure they were well known, and I would use the example of Service Tasmania matters because within Service Tasmania's policies and procedures there were a number of things that were already done, such as cash management and handling procedures. There are procedures for how you handle cash and audit trails around that and his suggestions were about ensuring they were articulated.

Some of the recommendations were around a fraud policy, which was developed and prepared in May 2012. We attached that to our submission and that is important because again, many of those practices were probably done, but having a policy then clarifies roles and responsibilities and ensures people know where to go. If we say to staff there is a fraud and corruption control policy, they cannot then say, 'I didn't know I wasn't supposed to do that', or a manager couldn't say 'I didn't know that was my responsibility'.

There were some recommendations around such things as password controls and policies to ensure they were better implemented. The fraud policy also refers to a number of other policies that happen, so there is not just one policy about improving our management of this. There is a number of things such as internet usage, credit card procedures, and a list of about 10 attached to the policy. It was about collating and emphasising where they were in the system and ensuring people knew what their responsibilities were. They are probably the key practices and other things continue to be done through our internal audit program, such as regular audits.

Ms FORREST - On that point, DPIPWE responded in quite a timely manner here because that policy is comprehensive and it was in May 2012 not long after he made his report. I note that recommendation 4 said that all entities should review and amend their corporate plan at least every two years. He said the review of the finance branch in 2014 did not recommend any changes to the policy. Was it only the finance branch that looked at this or was it broader than that? The policy would not just affect people working in the finance branch.

Ms KENT - No. When we do a review of any corporate policy the usual process would be that someone would take the lead on it, in this case finance, and they would work closely with all the divisions, usually through a business manager. Most divisions have some sort of business manager role and then the business manager themselves would say, 'My ILS division would probably have brought that control policy to our management team', and we would have looked at across each branch. It is like an escalating effect and then they would get feedback and the finance branch would collate that. Adrian may like to add to that.

Mr PEARCE - We use a consultative approach, so for any change to a policy we seek endorsement from all the divisions so when it finally gets to our senior executive for -

Ms KENT - Signing.

Mr PEARCE - Yes - everyone is on the same page. Consultation is a big part of our process.

Ms FORREST - What sort of feedback did you get from staff across the board on the policy when it was first put in place in 2012? I accept that consolidation things were probably already happening but it is important to have it in the policy, as you said. Then again during the review period, what sort of feedback was there from management right down?

Mr PEARCE - I wasn't part of the process that implemented the policy so I can't comment exactly on the feedback. A draft policy is put forward and then all managers have an opportunity to amend, provide suggestions to that policy and they are taken into consideration when doing the final version. Regarding specific feedback, I can't comment.

Ms KENT - I can probably comment. Back in division land, if I had been the general manager when we received it to comment on I think we found it was really useful to clarify roles and responsibilities of people to make sure everyone knew what their position was. One of the recommendations, as you know, from the Auditor-General was to have a specified board corruption and control officer in an agency. Our agency, as we said in our response, determined that it would not just nominate one person but we would in fact ensure it was every division head, so that is the general manager-level person like myself. That ups the ante, I think. It is better to have nine people or more considering it is their role. That was a useful process and it is useful for people to know that is where they go if they have an issue or concern. If an individual staff member thinks someone might be doing something that is not right they know they can go to someone directly. I think they were the main suggestions or comments around clarifying what to do in that.

The other comment was around what fraud is and the policy was useful in outlining all the range of things fraud could be. It is really easy for people to just think, 'I've never stolen any money, I wouldn't do that', and not think about the other things fraud can be, for example misuse of resources, not putting in a leave form or whatever. From my recollection when we had those initial discussions I thought they were the more important things to make people see there are many things that constitute fraud, not just the big example you see in the papers when someone has defrauded Centrelink for hundreds of millions of dollars. It is a better concept about what it is to be a public servant and these are all the things we are responsible for ensuring we do not do.

Ms FORREST - In that regard, has there been an increase in the incidence of recording fraud or concerns about fraud since the policy has been in place?

Ms KENT - We probably don't have the numbers in terms of what is on the register about what has been reported or investigated prior to 2011 but we can take that on notice if you like and I can clarify in terms of numbers prior to 2011.

Ms FORREST - That would be helpful.

Ms KENT - Post-2011 and post-2012 of the policy we keep a register and there are four or five instances of what we have been investigating. In this case it is probably around money, I would have to say, as opposed to all those other ones that might not be listed as an incident yet. I think that is maybe one of the areas where we are still developing so it is hard to say whether the numbers have increased pre or post the policy.

Ms FORREST - You are talking about the senior managers' roles there. In recommendation 9 the Attorney-General recommended that all entities ensure that senior managers include

fraud management as a required responsibility, and the comment here is, 'It is not considered feasible for Human Services to update the individual statement of duties for every senior manager'. That sounds a bit odd and I would like you to explain that more. I am wondering how difficult it would be, particularly if there was a broad template. The rules are pretty much the same, regardless, I would have thought, so I am interested in why you think it is not feasible and why that hasn't been done?

Ms KENT - It is probably in the context of talking about your major duties; it certainly talks about how you need to behave. Most SODs have a general comment around meeting the code of conduct and the principles of the State Service Act, so I guess there would be a consideration that because you are expecting that of your employee and you as the person signing on to the statement of duties, that the fraud policy is like many other aspects of corporate policies you are expected to implement and uphold. I will use the example of work health and safety. Statements of duties reflect some of that. I take it on board that it is a recommendation that has been made and I guess it is one of those ones where you keep thinking it is a work in progress. What do you include in a SOD, do you look at all the corporate policies you expect everyone to implement?

Ms FORREST - Isn't it simply a matter of linking a requirement to abide by the fraud and corruption control policy in the statement of duties? The way I read that is that is all the AG is recommending so I find it odd that that would not be part of it when it is such an important aspect.

Ms KENT - I take your point. I think we are making the assumption it is part of it, as are all the important policies we are expected to do as a senior manager. I guess the corollary would be, given my comments I made around the ex-division heads - the fraud control and corruption officer - that that may be how we do it, so that each of the GM SODs have that specific role included in them.

Ms FORREST - He is talking about senior management SODs.

Mrs TAYLOR - I have an overarching question. Your responses are good and you have obviously acted on many of the things the Auditor-General recommended, so if the Auditor-General was to come back and look at you now, are you satisfied you have addressed pretty much everything? What are you still working on or not quite satisfied with? What do you think the AG might not be happy with?

Ms KENT - I think he would be happy. He is always doing audits on things I would consider to be semi-related to these things. A current one he has under way is around ICT security, for example. We constantly feel we are being audited by him in different ways, and with many of them the principles are the same and the issues might just be around the content, as opposed to the context. I think he would be reasonably happy that we are addressing all the issues. Whenever he makes a recommendation we certainly look at it and consider it further. In nearly all cases we either take it on board or do something very akin to that, if not exactly how he has suggested, so the how might change but the principle does not.

We have ongoing audits. We have internal audit program and ongoing processes within each of our workplaces according to their risk and how that needs to be managed. Using Service Tasmania as an example, we see that as very much an area that has to have a constant program of audits, and high-level audits and spot audits are done all the time on cash-

handling procedures, for example. My assessment would be that the Auditor-General would be confident we are addressing what he required and more.

Mrs TAYLOR - It is related to the question of our role as much as anything; we are now looking at audits that were done in 2010, 2011 and different departments have responded differently and we don't seem to have a way of checking at the moment. We are just thinking about how do we check maybe a year or two later that the Auditor-General's report has been taken on board by any agency.

Ms KENT - We would like to think that we would have a process by which his recommendations would always be picked up, considered, and then assessed and reviewed. I would say through a general agency program of internal audit when we're looking at that we are both identifying what we see as our own risks and how they need to be managed, what the Auditor-General is saying and what an independent external auditor might say as well, and where there might have been other actions in another place where we have then needed to address those. I feel we would be practically trying to do that all the time.

I am not saying we are doing everything perfectly all the time either, because I think these opportunities give us a chance to say, 'Ah, we did do that, but did we do the next step?' I think the question just asked, for example, around the SODs, prompted another thought of how we might be able to assess those. We talk about excessive leave balances, we talk about a whole range of other, what I would consider, day-to-day work and we are constantly trying to work out how to do that better. I would be reasonably confident.

Mrs TAYLOR - Can I ask then, because there does not seem to be a generic process, but when you receive the Auditor-General's report, what happens to it? How do you process it? It comes to the Secretary, I guess, and then what?

Ms KENT - I think in these cases - and I haven't been on the Internal Audit Committee now for over five or six years - but it comes to the Internal Audit Committee, so they put that. That is chaired by the Deputy Secretary in the agency and has another senior member of the executive on it and an independent person - someone from outside, an external person. Adrian and others, someone from the policy area, acts as the executive officer to that. Adrian, through his finance role, inputs into that. There is that group, and I think it is the best governance for these sorts of reports. If there were many recommendations, for example, and it looked like we hadn't addressed them, then I think that would demonstrate that needed to be part of the internal audit program.

Ms COURTNEY - That was my question anyway.

Mrs TAYLOR - For us that is important, understanding how the process works and we might make recommendations about how that might happen in the future.

CHAIR - Just going back to earlier when you were talking about your policies and how you know that the policies have been read, that is one thing; but how do you know that they are being understood? How is that process taken or adopted?

Ms KENT - That is done at a range of levels and probably where the focus is - I think you change your focus according to the group of staff that needs to know. I will use Service Tasmania as an example again, and we answered it when we talked about recommendation 8

about how all employees have a general awareness. Two things have happened: all new staff members to our agency have an induction, both an induction with their manager but also a half-day session that is organised through HR. That includes the Secretary, the Deputy Secretary and others all speak at that. In one of those sessions in that half day, in fact John Whittington when he was in his Deputy Secretary role used to run a session called 'What it Means to be a Public Servant' and that would articulate a range of these policies. Then when you have started your job, your manager is responsible for ensuring that you are constantly inducted into what new policies you might need to know about. That is a day-to-day process. Then when you do your performance management review annually - at least annually because you might have two a year if you were a Service Tas person doing cash management all the time as part of your three- or four-week training that you do, there would be a whole section on cash management handling and what is required. They would emphasise that issues around password control are important and how you link information and share information, and those sorts of things.

They would have a stronger emphasis in somewhere like Service Tasmania. They would probably have a stronger emphasis in somewhere like the parks visitor centres where there is also cash handling. I guess that depends on what your role and task is. You might just get a very generic overview or you might have very specific training around aspects of your job that require you to do these things. In Service Tasmania again, you have QAs. There are actually positions called QA officers and part of their role is to ensure that people know what they are doing and 'Have you read that policy?' and 'Do you know what that means?'. It is more of a hands-on, like a manual. It is about 70 pages on cash handling. You need to be working on it every day, it is not something you read like the rest of us can - on the internet, and I will go to it when I need it. Some deal with it every day. It is a bit horses for courses depending on what your task is in that broader sense. Managers would then need to determine whether you need to be reminded more about your role - if you will have delegations, for example. If you are a supervisor or manager with set delegations, and you are signing off on someone's travel claim form, do you know what you are signing off on, and what you are checking for?

Ms FORREST - Recommendation 12 says 'all entities should perform police checks of senior or higher risk positions and document background checks for prospective employees'. In your response you talk about all higher risk positions within Service Tasmania are required to satisfy pre-employment national criminal history police checks, what are you referring to with the higher risk position?

Ms KENT - In fact all Service Tasmania staff have to undertake police checks now - customer service officers -

Ms FORREST - Has that changed recently?

Ms KENT - Yes. There has always been - not always, that is not quite true - all CSOs - if I can come back to you with a written clarification around the Service Tasmania officers but they we are required to do police checks as part of our delivery of services for Centrelink. There had already been some requirements to deliver - I am almost certain that it is all Service Tasmania staff but I may need to clarify that for you - not just higher risk.

Mr PEARCE - In addition, all finance staff have a police check and I believe HR payroll as well.

Ms KENT - I will confirm with you about the Service Tasmania CSOs but my understanding is that we do police checks on all Service Tasmania staff now. I will double check that.

Ms FORREST - You have touched on this and gone around it a bit when I asked you earlier had there been an increase in instances of fraud. When you provide that information later, I would be interested, as a result of any of those instances - not any specific ones, but in general terms - have other requirements or policies changed as a result of those? Have they identified a gap or a flaw that has enabled that to happen? Part of that is really understanding what fraud is as you have already described. In that area, has there been a policy change and what has been the response of people who have undertaken - do they do a training module or anything around the policy, or is it just an expectation they will read it? What has been their response to that?

Ms KENT - In Service Tasmania they would do specific training around how to do certain things, all the components of the policy; I have mentioned the cash management one. In terms of the responses to the couple of incidents I have been aware of and involved in, they have demonstrated that the system's controls have worked. In the couple of cases I know about in Service Tasmania, the system has identified that something has gone wrong, so in fact it has been quickly picked up where someone might have done something wrong. There has been another case where a fellow employee thought someone was doing something wrong in handling cash properly, raised that with their manager, so it is going to be raised with me, et cetera, and a process was put in place to investigate. They all demonstrated that the policy worked and that there were systems in place.

Another one was where they did what is called a random audit, but they are not that random, they are done on a rolling basis of cash handling, and an audit picked up quickly there seemed to be discrepancy in a till, for example, and that is done all the time and in that case, investigated further and determined that there did seem to be differences in information being provided.

All three demonstrated that the processes and systems worked and were good examples to be able to say this is what we do, this is how we do it and this picks up the problem and can rectify or address it.

Ms FORREST - In terms of the cash handling, in some respects it is a little easier to check because if a till does not add up it is obvious pretty quickly if you are checking on it as you say your internal controls do. What about the other areas that are not cash-related or money-related?

Ms KENT - They are the ones where we don't necessarily have good ways of recording where those incidents have occurred. Most of the emphasis has been on instances of fraud in terms of cash in terms of their fraud register. The others probably get caught up in a whole range of other things and they will be addressed and investigated but it may not be talked about as fraud.

Ms FORREST - In terms of informing your staff from management right down, can you step through that process? Obviously the policy is there and that is great, but does it just link back to the expectation that people will read it or are there ongoing information sessions or workshops of anything like that to inform people of what we are talking about? The prime

thing is awareness. Most people identify fraud as money and do not look at it as things in terms of monetary value.

Ms KENT - It is emphasised through day-to-day operations. It would be one aspect of a footnote. It would be around constantly checking that everyone was confident they were doing travel applications properly or that credit cards have been reconciled properly. There is a constant work program to look at different aspects, like excess leave balances, for example. Every quarter or so - even more often if we wanted it - most of us as managers could get a printout of where we have staff with excess leave. If that demonstrates you have staff who have not taken leave who might be in positions, as the Auditor-General said, where they are part of managing a system that could possibly be doing things they should not, then that is an issue you should be looking at anyway, other than the fact that people should be taking their leave. It is built in, it is embedded in all aspects of what you are doing in terms of delivering your corporate services. Those things are reviewed more regularly.

Mr PEARCE - There is also a lot of other mechanisms regarding air travel and credit cards. Our finance branch does a compliance review each year and highlights if there are discrepancies with that so senior management will see those individual cases and then they will go to the business manager of the employee. With things like excess leave balances, reports go out so people are very aware of that and it would be acted upon.

Ms KENT - Internet usage, for example, gets picked up in another way. The IT section would be looking at the top 10 data usage and if someone is appearing on that list constantly, they look at whether it is appropriate, if they realise what they are doing, if it is all work related or not. The checks and balances are throughout our day-to-day work. Probably don't talk about fraud and corruption control necessarily as the overarching policy all the time but the components we do every day are part of that. In terms of how we can reiterate that, I am happy to take advice on whether you think it should be more reiterated.

Ms FORREST - We spoke to DHHS earlier and they have an e-learning module that all staff are required to do under the provision of their manager.

Ms KENT - I am the department's rep on the Integrity Commission's ethical reference committee and they are trying to put all their modules into an e-learning process as well. I agree that is often a quick way to remind people to check a policy because most of them don't want to trawl through the intranet looking for policies.

Ms FORREST - Remembering to do it, too, is one of the things. It is part of an expectation - I assume you did performance reviews and part of that is that you have participated in this e-learning modules. It is awareness that is important for people in terms of fraud, particularly those non-direct cash things, the monetary value issues that often people don't realise. If it is brought to their attention on a regular basis, it is more likely to be effective.

Ms KENT - I agree.

Ms FORREST - Is there any likelihood DPIPWE will look at implementing those sorts of approaches to enhance this area?

Ms KENT - We are always looking for ways to enhance training and development because we know can't continue the old-fashioned ways of taking people out of the workplace for

days on end. The e-learning modules are good and we have done that with a few other training modules around WHS. That was a quick way because, again, with the new change in those laws last year, every staff member had to be aware of what the changes meant. We did that through an e-learning module that everyone had to do. If you didn't do it, it was recorded in a way that we could know as managers. This would be a good example of where we could do it with this and more corporate policies.

CHAIR - We sent you a questionnaire which prompted the answers we received back. What impact did that have on you? Did it cause you to go back and check up on the all the AG's recommendations to see whether you had met them? It seems to me there is a flaw in the system inasmuch as a department is not required to go back to the AG and say, 'We have addressed these recommendations, this is how we have addressed then, and we now have all these new things in place'. What impact has this had on your department?

Ms KENT - It was coordinated through the internal audit committee and I recall it went back to those business units that were most impacted, such as Service Tasmania and the Corporate Services division. I believe we did most of the responses and it was a useful way of flagging back with those areas about what we did or did not do and if we still had things to do. If we thought there were still some gaps, he would provide us with a bit of a checklist of things we needed to articulate, similar to his other reports.

Mr BACON - Was the questionnaire worthwhile for the department?

Ms KENT - I think it is always worthwhile for us to check we have done something or not - and if not, why not.

Mr PEARCE - The audit committee is the one that manages these and will ensure everything is being actioned so if they were failing their duty they would have a problem.

Ms FORREST - I would like to commend DPIPWE for getting onto it and doing a good job in this area.

Mrs RYLAH - I am equally impressed. I thought it was very well done and comprehensive.

CHAIR - We appreciate very much the way in which you have answered the questions today.

THE WITNESSES WITHDREW.

Mr MIKE BROWN, CHIEF OFFICER, STATE FIRE COMMISSION, AND **Mr TODD CRAWFORD**, DIRECTOR FINANCIAL AND PHYSICAL RESOURCES, DEPARTMENT OF POLICE AND EMERGENCY MANAGEMENT, WERE CALLED, MADE THE STATUTORY DECLARATION AND WERE EXAMINED.

CHAIR - Before we commence, this is a public hearing we are having here today. It is being recorded on Hansard and will be available publicly. If at any stage you reach a position, and I doubt that you will, where you think you should talk to us in confidence, in camera, then please put the question to the committee, or to me, and the committee will make a determination on whether we should go in camera and or not.

As you are aware, this is a follow-up of the Attorney-General's report that was issued in 2011 in relation to fraud control, which we have taken up and we have asked a number of questions of your department, Mike, and we have had a response to those questions. Now the committee is in the position where it wants to ask a number of questions to find out more about it and to see where it is going and what is happening in that area. We will go to questions in a moment.

Parliamentary privilege does apply here but once you walk outside these doors it no longer applies.

I will give you an opportunity at this stage, Mike, to make any statement or any comment you would like to make on the reply you provided to us or on any other issue around the Auditor-General's report of 2011.

Mr BROWN - Thanks, Mr Dean and members. The things we have done particularly since 2011 for the most part are reflected in the work we have been doing with the Department of Police and Emergency Management as a whole agency. Since that time we do have an agency or an organisation that looks after audit controls, including such things as fraud for the whole Department of Police and Emergency Services, which covers Fire Service and also Forensic Services Tasmania and State Emergency Services.

The other significant matter is that TFS has taken on a major obligation and a major body of work in institutionalising TFS values. Like lots of organisations we had a set of values, but they were not really known by a lot of people, but in underpinning the leadership development work that we have focused on over the last two or three years, I thought it very important that we really get people to have some input into our values. There are four values and they are around service professionalism, integrity and consideration. One of those values, in particular under integrity, is about being trustworthy and ethical.

CHAIR - Mike just tabled a document in regard to that.

Ms FORREST - What is that document, Ivan?

CHAIR - It is called TFS Values and it is on the point that Mike was just making to us then. It is a one-page document in dot point form covering those areas: service, professionalism, integrity and consideration.

Mr BROWN - In light of that we wanted to make sure that it was something more than just a poster on the wall. It has informed a lot of work that has been happening across all work groups and volunteer groups about how to act out those values and ensure that they are fully understood and institutionalised. While we don't, in such things as perhaps statements of duties or even induction programs, specifically mention fraud in itself, it is certainly covered under the umbrellas of that key value of integrity and the requirement to be ethical. It is certainly addressed under professionalism as well, in order to be accountable for our actions.

Ms FORREST - I have a couple of questions, Ivan. Mike, I'm just going through some of your responses here that you have provided and to the first recommendation that you should adopt a fraud definition and develop a statement of attitude to fraud and communicate the fraud definition statement about attitude to fraud to all employees. You have talked about how you will adopt a fraud definition and develop a statement of attitude. Has that happened?

Mr BROWN - At this point I might hand over to Todd. Todd represents the broader organisation on our Internal Audit Committee where we work with our internal auditors, Wise Lord & Ferguson. If it is not adopted already, it is most certainly a key intent.

Mr CRAWFORD - No, it hasn't been adopted at this point in time. The audit committee of the Department of Police and Emergency Management has recognised this recommendation as being crucial to the operation of TFS, but more broadly within the Department of Police and Emergency Management there is no specific definition of fraud or a statement of attitude to fraud. We have, within the next couple of months, a renewed second stage of our strategic audit plan process, so we have had a three-year work plan that has just completed and we are, at an executive level, planning for the next three years of work for our internal auditors. In discussions with the Chief Officer and the Secretary, we have determined that obviously fraud should take a key focus in that work plan into the future. We will be engaging Wise Lord & Ferguson to develop that fraud control plan.

Ms FORREST - I am interested that the Auditor-General, in his report and the outcome of his inquiry in 2010, reported in 2011 just after that, and it is now 2015. It has taken an awfully long time to get to this point. You say it is a crucial and key issue, so why has it taken so long?

Mr BROWN - It was that we considered we were going to be very much covering fraud and things like gift registries, and all sorts of things around where there are possibilities of indiscretions under our values. Being a big organisation of over 5 500 people with all the volunteers, too, we certainly wanted to take a broader overview, but be inclusive of fraud within it. While it is not specifically mentioned, the focus was on covering it under the work that we were doing around our values.

Ms FORREST - The cynic in me can say that you got the Auditor-General's report and did not really do anything until you had a subsequent inquiry from the PAC - that's us - to progress this. Is the cynic being cynical in that?

CHAIR - I guess the question is if it is right that you left it until you received our report to do something about it?

Mr BROWN - I don't think so. I am trying to think of timing on this but it was before 2011 that we started to work on developing our values, and that was a big program in itself. That took about 12 months because we needed to take vertical slice groups right across the organisation to have input into them. We were not going to impose the values on the organisation, we wanted people to have input into what the values were. Our obligations around being ethical and being a public authority needed to be front and centre and that is why the value of integrity is there and why we were very insistent about it including ethics in a more broad sense, not just specifically fraud.

Ms FORREST - Did that work start in 2012 on the values and ethics?

Mr BROWN - No, it would have been prior to that. I suggest 2008 to 2009.

Ms FORREST - So it was already a work in progress prior to the Auditor-General's report?

Mr BROWN - Yes.

Ms FORREST - I appreciate it can take a while and you would want to take the whole organisation with you on something like that if they going to adopt it, it just seems to have taken a long time since the clear recommendation was made by the Attorney-General in this area. It would be good to have a timeline of what you done when, if you are able to provide that? Not right now but maybe later to the committee.

Mr BROWN - Certainly.

CHAIR - You can take that on notice and provide that later. We will write to you with any issues that are outstanding after our session today.

Ms FORREST - You have noted in regard to this recommendation that DPEM will adopt a fraud control plan which includes the Tasmania Fire Service. Has that been adopted where is the fraud control plan at the moment?

Mr CRAWFORD - That would on the agenda for the coming work plan for the audit committee. That is part of the strategic audit and risk management framework.

To take a step back in terms of time frames it may answer the previous question. TFS joined the department's broader audit committee in May 2011, so in terms of timing it was just after this report was delivered. There was then a series of strategic audits undertaken, some of which had a specific focus on financial controls vis-a-vis fraud-related activities. Those outcomes at an operational and policy level are being actioned. The contract for internal audit services has now been renewed, we are in a planning phase for the next three years of that contract and we would see the fraud control plan development falling into that timeframe as a priority.

Ms FORREST - Is that work being done by Wise Lord & Ferguson?

Mr CRAWFORD - Under the auspices of the department's audit committee.

Ms FORREST - By Wise Lord & Ferguson?

Mr CRAWFORD - It will be done by them in the future. They have been engaged to prepare an agency-wide risk management framework. In terms of governance, we have an audit committee in place, we are developing an agency-wide risk framework within the context of financial risk and fraud will form a component of that. We see a fraud control plan being the next layer of documentation within that framework.

CHAIR - Ruth has made the point of why it had taken so long to put these things into place because when the report was released in 2011 the Auditor-General identified to you the need to have a fraud control plan in place and yet four years later you are simply saying now that you are going to put one into place. The Auditor-General could feel a little concerned about that, as does this committee. You cannot take that any further? You have provided an answer as to why you have not gone down that path, so when you say it will be done now as a priority, when is it likely to be finished? When will we see it?

Mr CRAWFORD - That work would be likely to occur by the end of this calendar year.

CHAIR - That is what you are aiming for?

Mr CRAWFORD - There are no other plans other than the risk management framework. There is nothing on the strategic audit agenda at the moment, so it is the number one priority beyond that.

CHAIR - When the AG provided that report in 2011, I take it comes to you, Mike, as the chief of TFS?

Mr BROWN - Yes.

CHAIR - You would have received that report, so where did it go to from there and what priority did you see on those issues raised by the AG that needed some attention by your service?

Mr BROWN - I raised it most certainly with the executive leadership team of Tasmania Fire Service. It wasn't until a little later in 2011 that we had the whole-of-department committee work on that. There was a lot of consideration by the executive leadership team that we needed to address fraud, but under the broader umbrella for the moment of our values and ensure that was in the planned discussions that happened with work groups, embedded in induction programs for volunteers and staff right across the board, and ensure from the point of view of being accountable that we were acting on anything that had even the potential for fraud. We wanted to look at that in the broader sense because there were all sorts of other financial risks that might include gifts and benefits, predicated use for senior officers et cetera that we needed in the beginning to at least get some umbrella framework around the expected behaviours about being accountable for public moneys.

CHAIR - What involvement did the Secretary have in this process? It would have come, I guess, from the Secretary down to you.

Mr BROWN - In this case it didn't; it came straight to me as the head of the statutory authority, the Tasmania Fire Service.

CHAIR - At what stage was the Secretary of DPEM made aware of that report coming to you?

Mr BROWN - I can't recall. It would have been at some point out of the priorities and work that were being put before the departmental audit committee.

CHAIR - The reason for that question was to ascertain whether the secretary of DPEM was simply getting feedback from you as to where you were with these issues, but if you are not certain when he got that, that is probably not a question you could answer.

Mrs TAYLOR - The process says you would have sent it to your audit and risk committee.

Mr BROWN - I can't remember when in 2011 we got this report as compared to when we started up on the internal audit but it would have been around that time.

Mrs TAYLOR - Is that what you would normally do as a process now?

Mr BROWN - Yes, it would be.

Mrs TAYLOR - One of the things we are looking at, Mike, across all the departments, is what the process is when the AG does a report and what happens to it. It obviously goes to the Secretary of a department, one presumes, and we are trying to establish if there is a pattern as to what agencies then do with it and how it filters down.

Mr BROWN - It is fair to say it is now more formalised. I think the relationship around Fire with the Department of Police and Emergency Management in a broad context is now more formalised and that would be a logical place for Auditor-General's reports to go to.

CHAIR - I am looking at the comment here that the TFS is now implementing the recommendations from these reviews and as part of a broader DPEM environment will adopt a fraud control plan. Is the fraud control plan we are talking about going to be developed now on a whole-of-department basis - Police, Fire Service, Ambulance - not specific just to the TFS?

Mr BROWN - No.

CHAIR - So Police have a big role to play in bringing that together as well?

Mr BROWN - Yes.

CHAIR - What team is putting that together? Is it a combined team of Police, Fire Service Ambulance and SES?

Mr BROWN - The audit committee comprises representatives from each of those disparate work groups under DPEM.

CHAIR - The reason I ask is that DPEM, from my own knowledge, had fraud plans in place probably forever and a day on their own organisation but now it is a redoing all of that to encompass all three emergency services.

Mrs TAYLOR - If the Auditor-General were to come back now, looking at the original audit in 2011, there were only two satisfactory ticks in the suitable management strategy for fraud and lots of 'to be improved's; how would you score now?

Mr BROWN - A lot of the ones around IT controls certainly have been strengthened. We have policies in there now about refreshing such things as passwords, and there are now a lot more controls around server locations and security.

Mrs TAYLOR - Cash is better controlled than it was?

Mr BROWN - Absolutely. Electronic transfer has improved, as have the accountabilities against credit cards. There have been some major improvements in those systems-type processes.

Mrs TAYLOR - I hear what you are saying, that you have included fraud as part of a bigger review, and that is fine. I suppose that is what the Auditor-General was looking for, to make sure specifically those things were addressed. Even if it is part of a bigger whole and you have addressed the issues, it probably would be useful if you highlighted some of those - took them out, if you like, and put them in a fraud control policy.

One of the things was that TFS will introduce police checks for senior and high-risk positions. Does this mean you do not currently have police checks?

Mr BROWN - We have police checks now across the organisations right through, including for volunteers. The level of scrutiny around all people in the organisations is increasing a lot. We are going through the new one at the moment about oversight and care of minors and children in organisations. We are taking our accountabilities around that area more seriously and there is an increasing level of awareness around that. There is an increasing level of need for compliance around that.

Mrs TAYLOR - You have addressed that, and that is good.

Ms FORREST - With regard to recommendation 9 around the senior manager's statement of duties, it says here Tasmania Fire Service was considering introducing into its senior management statements of duty fraud management responsibility. Has that been done?

Mr BROWN - It has been done again and the emphasis has been put on the organisational values and the fact that everyone will be judged by, and be held accountable to, those values. That is the way it has been dealt with. The back part of the statement of duties is getting huge in terms of all the sorts of things it needs to meet and if we were to put fraud in there, credit card control, gifts and benefits all specifically, it could be lost in its intent, I think, so specifically it is not there.

Ms FORREST - If you are going to adopt a fraud control plan, surely that will deal with gifts, credit card use and other aspects of fraud or potential fraud; wouldn't it be appropriate for a statement of duty to require compliance with the fraud control plan? Simply that because that would encompass it and sit very well with your values.

Mr BROWN - That could well be the outcome of the development of the fraud control plan under the DPEM audit committee.

Ms FORREST - Is that something you will consider? This is a very clear recommendation that it should be very clearly part of the senior management statement of duties. Whilst you can say it is all linked to the values, the values overarch the whole position anyway, not that their statement of duties apply to everything.

Mr BROWN - Sure. The other point to make is that it brings it right upfront in the statement of duties about adherence to the Code of Conduct. The State Service Code of Conduct is quite implicit about the seriousness that fraud control has taken across the State Service.

Ms FORREST - Hence the suggestion that it should be in their statement of duties as a standalone item. It is what the Auditor-General is suggesting.

Mr BROWN - We will have to take that one on board then, but then point out that it is in consideration of quite a number of other things as well.

CHAIR - Just before we get away from that, in your responses immediately above that it seems to me that you will do certain things, but it would seem to me, from my observation, that you probably haven't done that much because above that you have 'TFS will include fraud awareness in its induction program (time frame).' What you are saying is that you will do it. Have you done it? Is it now a part of the induction program?

Mr BROWN - In the reinforcement of the values around ethical behaviour and being accountable, we consider it has been addressed in there. With people who work in financial areas specifically, it is more implicit in terms of their induction program. Induction programs aren't the same right across the organisations, they are tailored to the areas where the people work in. Certainly for those who work in financial management or even handling cash, it is made more implicit in their inductions.

CHAIR - Okay, it's more focused if you have people working into those areas. But for a new recruit starting within the Fire Service, what sort of an induction program do they have in relation to fraud control within the organisation, is there any component of the training curriculum?

Mr BROWN - There is most certainly around expected behaviours, again reflecting on the values. What is in their program at recruit level about fraud specifically, I am unaware of, Mr Dean.

CHAIR - You might be able to take that on notice if there is anything in that area, seeing it is a very important matter. Take it on notice. We will write back to you anyway and put these points to you so it is clear on which issues we are still to receive some information.

Ms FORREST - You also note, Mike, that there will be a review of the current risk register and you seem to be saying in the comments that that has been part of this ongoing work with Wise Lord & Ferguson. Has it actually occurred?

Mr BROWN - It has, Ms Forrest. We have had that as part of the State Fire Commission's standard agenda item on a regular basis, to do a review of our current risk register. Moreover, as a broader department, it is most certainly a priority for the audit committee to

do a larger whole-of-organisation register work. In terms of governance we consider it is something we need to get back to and give some more focus to.

Ms FORREST - I assume as part of that review there would be reporting against the risks and, in doing that, do you have any information about what issues have been identified, or has there been, for example, an increase in instances of fraud or concerns raised about fraud, whether it has been substantiated or not?

Mr BROWN - To the best of my knowledge, there hasn't been any increase in instances of fraud across the organisation. The State Fire Commission, as I said before, has on one of its regular reporting cycles the review of our risk register which covers a huge range of risks for the organisation, but including financial risk being inclusive of fraud potential as well, and works from time to time reviewing our protocols or procedures around financial management and fraud, and we are amending that from time to time.

Ms COURTNEY - We have been talking a lot about how fraud, for your understanding, falls underneath the TFS values. Did you say these have been used now since 2008?

Mr BROWN - They first started being developed around 2008, so it took probably 12 months before we had them fully developed.

Ms COURTNEY - My question really comes down to if these TFS values were being implemented and used in 2010 when the Auditor-General did the audit and the AG felt the theme of looking specifically at fraud control was not coming through in these values - and I understand your rationale that it fits under ethics and as a rational person, I would agree with that - if the Auditor-General in the past thought there was not enough focus or it was not clearly extracted and that was the case in 2010, I expect it would still be the case that the AG would suspect that if he did an audit now that might not be being clearly addressed through this framework, even though senior management may think it addresses the issues from a moral, ethical and integrity perspective. Perhaps it needs to be extracted further and specific training given to staff, whether it is in the induction training or whether it is specific management training. I know that is more of a comment rather than a question but it seems to me that the specific issue is not being teased out from these TFS values, at least not to the Auditor-General's satisfaction.

Mr BROWN - I can see your point on the timing but to get these out through an organisation of so many people has taken a long time. We are still having focus groups amongst different work groups, which could be anywhere from within the TFS store to a brigade on King Island as to what is being expected by them and having a discussion with them about what they should do. It is very hard to be measurable about what we have done in mitigating things like fraud, but we are, in an anecdotal sense, noticing that people are more inclined to report something because they know the organisation's values will support them in acting upon it. It has been effective, but to be measurable about that is somewhat difficult. Even if you had the best fraud control induction, it may not necessarily change the behaviour and attitude in approach.

Ms COURTNEY - One of the Auditor-General's recommendations related to the reporting mechanism available to staff and the TFS response is that the TFS considers there is already a clear reporting mechanism. It is almost as though the TFS is disagreeing with the Auditor-

General's viewpoint that there needs to be work done in that respect. What is your view with respect to reporting?

Mr BROWN - I didn't give that one a whole lot of attention myself. Was there a time frame difference from when the report came out to when we produced this? I think there was.

Ms COURTNEY - From when the Auditor-General's original report came out?

Mr BROWN - Yes.

Ms COURTNEY - That was in 2011.

Mr BROWN - What recommendation was it?

CHAIR - Recommendation 136.13.

Ms WOODS - The TFS response column would have been a response sought by the Auditor-General and included in his report as the entity's submission with regard to his recommendation at the time.

CHAIR - If you want to take that on notice, please do so.

Mr BROWN - Yes, I will take that on notice.

Ms FORREST - With regard to recommendation 12 about employment screening, you said you have introduced police checks for senior and high-risk positions and have a policy - 3/04 - for that. Are you able to provide us with a copy of that? You can talk to it briefly if you wish but it would be good to have a copy of the policy.

Mr BROWN - I am happy to provide the policy in that regard. We do police checks now for personnel at all levels, inclusive of volunteers. Managing police checks for 5 000 people is interesting.

Ms FORREST - How long has that been a policy position?

Mr BROWN - Looking at the policy number I would suggest it is from 2004.

Ms FORREST - If that was the case, that was well before the Auditor-General conducted his investigation to say you should perform police checks for senior and high-risk positions and have background checks performed. Clearly at the time it wasn't happening.

Mr BROWN - I will have to look at that in context because that might be around promoting people, which may or may not have been subject to a recheck.

CHAIR - Mike, we will put that on notice also.

Ms FORREST - In recommendations 27 and 28, which is about management of cash and corporate card use, there was some comment made about the reliability of the procedure you have in play, but there is still a risk, it appears, in small and more frequent episodes. You have controls to recognise and detect larger episodes of fraud, but most people when they

want to defraud someone in a monetary sense will do it with small bits to start with to see if they are picked up. Do you have processes in place to detect the smaller instances as well?

Mr BROWN - Yes, we have. For instance, with petty cash there are the normal controls that we find fairly common across government in all areas, that everything has to be reconciled with an appropriate receipt and signed off by a supervising person or manager. In regard to credit card use it is under the same control, so all receipts need to be produced. If they have been lost, that has to be subject to a statutory declaration being prepared and that has to be authorised by an independent or senior person.

Ms FORREST - Do you have credit limits set on those corporate cards?

Mr BROWN - There are, under the instruments and delegations we have across most government agencies. There are limits set at different levels.

Ms FORREST - With the reconciliation process, I presume there is a fairly regular one. How often does that occur and who is it done by?

Mr BROWN - It is done monthly on the reconciliation of the accounts that will come through from the bank. Each individual with a card must have receipts to support that and a reasoning and a cost code and must have it authorised by an independent, more senior person.

Ms FORREST - And that is the same with the EFT transfers and credit card transactions?

Mr BROWN - I can't speak so much for the EFT transfers.

Mr CRAWFORD - I believe that is the case, but we would have to take that on notice to confirm it for you.

If I can make a comment in relation to the work that has been done by the combined department, it is very strategic in its focus but we recognise this is an important issue. One of the reviews we commissioned was in relation to the Tas Fire equipment branch, which is a semi-commercial arm of the organisation, and the focus of that was to ensure we had best-practice policy and risk controls in financial management. We went through and had the auditors look at stock control, cash receipting and invoicing, and make a range of recommendations, that have all been addressed, to ensure we are at that standard because we saw that as an area with potential for fraud given the high volumes of cash they deal with.

Ms FORREST - Is the return of the corporate card done immediately on separation of the employee?

Mr BROWN - Yes, it is. There is a checklist that people go through on exiting the department and certainly the return and reconciliation check of that credit card is part of our exit process.

Ms FORREST - Have there been instances of incorrect purchasing on credit cards in the last four or five years you are aware of?

Mr BROWN - No, not to my knowledge.

Ms FORREST - Can you inform us if there have been?

Mr BROWN - Can I inform you if there have been?

Ms FORREST - Do you need to check that or are you fairly confident?

Mr BROWN - I am fairly confident.

CHAIR - If there is a change to that you will come back.

Mr BROWN - Yes.

CHAIR - We will note that.

Ms FORREST - With regard to Recommendation 29, it talked about developing a testing procedure to determine a regular schedule to test backups of your server. You mentioned earlier in your evidence that you had done some work on that, so how is that going, is the testing procedure all completed?

Mr BROWN - Yes, we are very satisfied with our processes now in terms of server security. There is a lot of reliance on computer infrastructure and there has been a lot of work done to ensure that is more robust, as there has been with such things as password policy, so all of us need to revise and remember a new password now each quarter.

Mr CRAWFORD - Once again we commissioned our auditors to conduct an audit of our IT system's recovery and backup procedures and that audit was very positive in its findings.

Ms FORREST - Do you each have a record of access to the server?

Mr CRAWFORD - The server room is controlled by electronic fobs issued individually, so yes, we would.

Ms FORREST - Just with Recommendation 30 - control of finance and expenditure in procurement areas, you did note that limited staff numbers limit the ability to segregate duties fully. Are you confident, in spite of that, that fraud can be avoided in this environment or is it still an ongoing risk?

Mr BROWN - I think this is one of the benefits we talked about as an integrated audit committee, that is, the Fire Service and Department of Police and Emergency Management corporate services will be integrating and this will give us some more capacity to have those functional needs met. I think it is going to be one of the advantages out of having that corporate services integration.

Ms FORREST - Do you agree that improvements could be made to enhance or improve compliance with internal controls in expenditure and procurement areas?

Mr BROWN - We regularly review our internal procurement procedures and, wherever possible, we are acting in accordance with Treasury guidelines in that regard. We have confidence in our arrangements on procurement.

CHAIR - Ruth, I have to draw it to a conclusion because we have the other witnesses waiting, so if we have any more questions we may need to come back. The committee will make a determination on that, and also when we get the answers to the matters taken on notice as well. Having said that, I thank you both very much for being here today. I know that you are both very busy people, but it is a matter of the process that this committee wanted to work through with the AG, so thank you very much for the way in which you have answered the questions and the information you provided today.

THE WITNESSES WITHDREW.

Mr DAVID CLERK, CHIEF OPERATING OFFICER, **Mr CRAIG BARLING**, CHIEF FINANCIAL OFFICER, **Mr ALASTAIR McDOUGALL**, DIRECTOR, AUDIT AND RISK, AND **Mr CHRIS SMYTH**, EXECUTIVE DIRECTOR, HUMAN RESOURCES, UNIVERSITY OF TASMANIA, WERE CALLED, MADE THE STATUTORY DECLARATION AND WERE EXAMINED.

CHAIR - Before we commence, I advise you this is a public hearing. It is being recorded on Hansard and it will be made available publicly when it is transcribed. If at any stage during your evidence, you wish to give it in camera then bring it to our attention and the committee will make a determination on that.

You are protected by parliamentary privilege while you are in here but once you leave this room there is no protection at all provided to you. You would stand alone if you want to talk about the issue.

This is a follow-up to the Auditor-General's report done in 2011 in relation to fraud control and this committee is following up on those issues. We have provided to you a questionnaire asking you to respond to a number of questions and you have done that. At this stage there is an opportunity, and I am not sure through whom we should be directing the questions, whether it is the four of you together or there is a lead role here or not?

Mr CLERK - Probably me.

CHAIR - Thank you. We will direct our questions through you. At this stage I will give you the opportunity to make any statement you want to make in relation to the answers provided or anything in relation to fraud control, any changes you might have made in the short time since this matter arose. If you could do that and then we will go to questions from the members.

Mr CLERK - Sure, thank you, Chair.

Firstly, I apologise for the Vice-Chancellor not being here today; he is in the Antarctic today.

Ms FORREST - What a shame.

Laughter.

Mr CLERK - I am the Chief Operating Officer at the university and have responsibility for finance, human resources, information technology, buildings, marketing and legal matters.

There are a couple of points to make upfront. Obviously the university does take the whole area of fraud control seriously. I draw your attention to the facts, or at least highlight some of the key elements, around our fraud control framework. The first is, we have established and have clear articulation around the university's fundamental values. We do have an audit and risk committee meeting five times a year which is chaired independently and is properly funded and staffed within the university. We have made, particularly over the last four years, significant investment in new and enhanced IT systems and infrastructure. That includes a substantial investment over the last 18 months in IT security. We have in

existence a control of fraud and corruption policy which clearly articulates expectations in respect of fostering an ethical culture and supporting the existence of fraud risk register. We have in existence a fraud control plan which is embedded within this policy, and the existence of fraud reporting and investigation procedure to respond to instances of possible fraudulent activity. We also have and refresh annually a three-year internal audit strategic plan, the current being for 2015-17, which incorporates elements designed to consider the fraud and corruption threat.

Since the questionnaire was completed in December we have continued to implement around the recommendations. There were two recommendations that were still outstanding at the time of the questionnaire. One was around password control, and we are in the process of rolling that out and close to having completed that, and the other was around the matter of appropriate police checks. It is already being rolled out now, I believe, and we are close to having that in place. That will be fully effective this year.

Mrs TAYLOR - If the Auditor-General were to come and have another look at you now, would you get ticks on everything?

Mr CLERK - We would be in a much better position than we were before. He would still see that the police checks policy has been rolled out and we are in the process of new people coming in being subject to that. He would see massive improvements around IT security. The university had underinvested in IT systems and security for a long time and a lot of work has gone into improving things. We have put in a new student management system, a new finance system, and spent around $2 million in the last 18 months on IT security, and that includes password control which we did not have before. It sound like an obvious thing to have but the university did not.

Mr SMYTH - We have just been funded for a new HR system which will help with the identification of people. It will have the capacity to better track those employees of ours who have undertaken police record checks and the working with children check requirements and will be phased in by the second quarter of 2016.

Mrs TAYLOR - Will you do that only for new people coming in or will you go back and do it for all your existing employees?

Mr SMYTH - For working with children we will have to do it for all employees, current and future. For policy record checks we are going through a process of identifying those roles in the hierarchy and for new ones in that hierarchy we will do checks and work our way through the retrospective application of that arrangement.

Ms FORREST - I note that in your response to the Auditor-General's report at the time, was that the university would implement all but two of the recommendations which it alluded to. Recommendation 2 says UTAS should development a code of conduct that defines expected behaviour for all employees. Your response to that was that you do not maintain a formal code of conduct, in contradiction to the comment that you have adopted all recommendations except for those two you are working on. You have a control of fraud and corruption policy which contains a number of elements to establish the university's expectation in respect of behaviour. Do you believe you do not need a code of conduct because that exists? The Auditor-General made it clear that he thought a code of conduct was necessary as well.

Mr SMYTH - In response to your question, I have brought with me the Fair Work Act and regulations which have the framework of employment regulations we are bound by. It has a number of specific descriptions in relation to behaviour and they include theft, fraud and assault in terms of what are deemed to be, under this legislation, serious misconduct and therefore in all other circumstances an employee can be terminated by.

We are also governed by a modern award and an enterprise agreement that applies to all our staff at the university. That has a detailed description in relation to conduct and misconduct, including for our academics research misconduct, which is also governed by a national code. In that context we have adopted the position that we are already fairly well covered as to what would be inappropriate conduct and behaviour.

Our focus for the last four years now has been on promoting the University of Tasmania's values, which pick up on a positive aspect of how our employees are engaging with us as part of the university community and, more importantly, demonstrating appropriate behaviours of respect, justice, et cetera. We regularly update our staff in relation to those values. In quarter 3 of last year we wrote to them individually with a copy of the values as other means of promoting the university's values.

I would take the position that we are already covered by codes of behaviour and we are trying to use our own methods in promoting workplace behaviour through our university values. We also have a university behaviour policy which picks up what is inappropriate behaviour.

Ms FORREST - I expect the Auditor-General's office would have been aware of these other codes and legal requirements you operate under. That being the case, why would he then suggest you need a code of conduct as well? Do you have any idea why?

Mr SMYTH - It was before my time. It is fair to say that I was around in the Tasmanian state government when we introduced a code of conduct as well, so I am familiar with the concept, purpose and intent. The Tasmanian Public Service wasn't covered by the Fair Work Act, and still isn't, so there is a number of things that are quite significantly differently in the operating environment and the regulation for employee behaviour. I believe it is a good idea but we are already covered by it.

CHAIR - During the assessment process by the Auditor-General in relation to this matter of fraud control there were a number of points that didn't meet his expectations when he carried out his audit of the university. Why was that so? Was it the fact that you had things in place and weren't updating them, or were there things that should have been happening that weren't happening? What is the explanation for that, or didn't you agree with what the Auditor-General was saying?

Mr CLERK - Again, this happened before any of us were working at the university, but in the four years I have been there there has been a big push in refreshing policies within the university. We have a four-year refreshment cycle of our policies. Many of those were out of date and had perhaps had that spin on that four-year period. I mentioned before the IT environment at the university and two out of three ticks for IT reflects the fact that our controls weren't as strong as they could have been. We have undertaken a lot of work to try to address that. But that was a reflection, I think, of the priorities around funding at the time. Regarding the payroll we got three ticks, so that was okay.

Mr BARLING - Regarding cash control procedures around the university, we are still in the process of trying to go cashless around most of the sites which is why that is still a work in progress. We are a lot closer to that right now. The new student management system we have just put in place really helps us in that regard. We have done a lot of work in the past six months to get to the cashless point. We have also done a substantial amount of work around our bank reconciliation, which was one of the Auditor-General's recommendations. The fact that we have adopted nearly all his recommendations shows we agree with his intent about improving our processes as well.

Ms FORREST - One of the recommendations is around management accountability, and you haven't explicitly included reference to broad management and senior management statements of duties. That was one of the recommendations the Auditor-General made for a number of organisations, so do you intend to include that in the statement of duties for senior managers?

Mr SMYTH - It is something we have contemplated. Our senior management contracts are, for obvious reasons, very standard across the organisation and they include a reference to the university's policies, procedures and values. Highlighting a particular policy as opposed to the other numerous policies that we have may, in fact, be counterproductive in terms of the emphasis we want to give on responsibility for all of our policies, and having ownership for all of the procedures that we have in place.

I was acutely aware of this particular recommendation. We have continued to operate the standard senior management contracts, which actually reference all of our policies, procedures, behaviour requirements and expectations of our senior managers.

Mr BACON - Do you mean it is still under consideration?

Mr SMYTH - We consider everything all the time, it is just the timing issues on some of those, but we haven't implemented them to date in terms of our standard contracts. We refresh them every 12 months and review them because things change and other things move in, so it is part of our parcel of things to look at.

Ms FORREST - I am not involved in the review of those documents and the amount of work required in that, but this was a recommendation made back in 2010-11 and you say you review them regularly; why wouldn't it have been put in the statement of duties as expected as part of their role?

Mr SMYTH - It is an expectation that all of our staff, but our senior management in particular, take heed of, follow, adopt and implement all of our policies and procedures, including fraud -

Ms FORREST - Fraud control policies.

Mr SMYTH - Indeed, as well as all of the other requirements that we have on our senior managers.

Ms FORREST - It is implicit then, is that what you are saying?

Mr SMYTH - Absolutely, it could be argued to be explicit, in fact, because it is -

Ms FORREST - All true. You are congruent then that senior managers, when they read their statements of duties, are aware that that is part of their role, to be aware of and alert to issues of potential fraud, and managing and controlling that?

Mr SMYTH - I am very confident that our senior managers are acutely aware of that issue, as well as all the other expectations in relation to modelling good behaviours, upholding the university's values and implementing all of our policies, both themselves and for their staff.

Ms FORREST - Thank you.

Mrs TAYLOR - I was going to ask about the cash, but you have already addressed that issue.

Mrs RYLAH - I was interested in the training that you have provided. I noticed that there were at-risk staff groups that were identified. Can you tell me whether they have received the training?

CHAIR - Which point was that on, Joan?

Mrs RYLAH - In regards to fraud awareness, there was a recommendation where some at-risk staff groups were identified. I am just interested to know whether those groups received the training that was recommended.

CHAIR - Do you have the recommendation number in front of you, Joan?

Mrs RYLAH - No, I don't.

CHAIR - The university staff are looking at it now.

Ms COURTNEY - It would be 8.

Mr SMYTH - It's 14, I think.

Ms COURTNEY - Number 8 is 'targeted training sessions for particular at-risk staff groups were undertaken'.

CHAIR - Are you able to answer Joan's question in that regard?

Mr SMYTH - I don't know, I will have to take that on notice, I just do not know.

CHAIR - Absolutely. If you are unable to answer it you can take it on notice.

Mr SMYTH - I apologise for that.

CHAIR - We will write to you, David, in your position, and put very clearly what was taken on notice.

Ms FORREST - On that point, do you undertake any specific target of training in regard to fraud management or fraud control to avoid fraud at a senior management level? If so, what does that involve and does it go further down the line?

Some departments have heard evidence that there are e-learning programs that the senior staff roll out to the staff under them to make them aware because some people think fraud is just about money but it is obviously broader than that. Often that comes down to people being informed of what fraud actually is, to understand it before they can apply a policy process to it.

CHAIR - If you want to take that on notice rather than make a guess -

Mr SMYTH - I can speak to certain parts.

CHAIR - Right.

Mr SMYTH - Our payroll team is regularly advised of issues relating to proper management of funds and proper application of electronic fund transfers, et cetera. There are checks and balances they have to undertake prior to running the fortnightly payroll. I can speak about that particular group specifically and give more information on that, but to take a broad brush across the university I would have to talk to some other senior managers about what they do for their own specific areas as well.

Mr BARLING - I can also talk to the money component. We are doing quarterly sessions which include all staff. Sometimes they are targeted to certain areas, sometimes it is a broad-brush approach where we invite everyone along to update them on new policies around managing our money - the cashless thing is on the agenda for the next quarterly update, for example. There are certainly a lot of areas from a financial perspective where we are updating staff but I think Chris is right, to have the whole gambit.

Mr CLERK - One of the other things we have done recently and introduced for the first time to the extent of this year is, for the purposes of signing off on our financial accounts, we have had all of our senior staff sign a fraud letter so they understand and recognise what fraud is. That was introduced this year and the extension has gone out.

Mr BARLING - Yes, that is right. It went to the entire senior management team, which comprises, I think, 21 people.

CHAIR - As a part of that process, do the staff sign off to say that has occurred? Do you have it documented, you can demonstrate it has occurred?

Mr BARLING - Yes, they do. They asked a lot of questions through the process, too, so they were informed and they were very much in contact with us through understanding exactly what that meant and what they were required to sign off and assert.

Mr McDOUGALL - I will make a comment about the internal audit function. Obviously the threat of fraud plays a part in framing up the internal strategy at the university. There are a couple of things that have been introduced since the time the Auditor-General undertook his report. We have implemented a controlled self-assessment process which really is management self-assessment of key controls to mitigate risks, including fraud. We have

implemented that across our key finance and administrative processes. That is a self-assessment. We do independently validate a sample of those responses. That is important from an educational perspective as it highlights the awareness and the need to maintain an appropriate framework and internal control.

Second, we have implemented some data analytic routines. So while the controlled self-assessment is looking at the front end, data analytic routines, particularly around AP, vendor master data and recently payroll, we are looking and interrogating the large volume of data to highlight any anomalies. Importantly, we are doing that behind the system administrator, so it is certainly independent and that is monitored by my function within internal audit.

CHAIR - Thank you.

Ms FORREST - I notice you have implemented a new finance system in regard to expenditure and procurement; that has not thrown up any issues or challenges, has it or is it working well?

Mr BARLING - No, the finance system was done about three years ago and was a very smooth process, particularly compared to the experience with our student system. The finance system is working very effectively and we have the procurement module and we are adding a contracts module to that right now. It has been a very good system, from our perspective. It was a success - that is the only way to describe our finance system implementation.

CHAIR - Those are the issues the committee was concerned about. Thank you very much for your attendance today and for the way in which you have answered the questions. We will write shortly in relation to those couple of matters taken on notice so that will come through to you. The committee will then have a look at that and make a determination on where we should go. There is always a chance that we invite you back or ask further questions.

We appreciate you are all very busy people and giving the time to be here.

THE WITNESSES WITHDREW.

Mr ROBERT WILLIAMS, DEPUTY SECRETARY; **Mr MAT MOORE**, MANAGER INTERNAL AUDIT; **Mr KANE SALTER**, DIRECTOR FINANCE AND BUSINESS SERVICES; AND **Mr MARK WATSON**, DIRECTOR, INDUSTRIAL RELATIONS, DEPARTMENT OF EDUCATION, WERE CALLED, MADE THE STATUTORY DECLARATION AND WERE EXAMINED.

CHAIR (Mr Dean) - Welcome, gentlemen. This is a follow-up to the inquiry that was completed by the Auditor-General in 2011 in relation to fraud control. This committee is now following up on the issues that were raised by the Auditor-General, and in particular the recommendations that came out of that inquiry. This is a public inquiry that is being recorded and will be provided publicly. If at any stage during this session you would like to give evidence in camera, please identify that to the committee and we will make a decision and proceed accordingly. Parliamentary privilege applies in this environment but once you leave it no longer applies so you stand alone on anything you say on this matter outside of here. You have provided answers to the questionnaire we sent out, Robert, but is there anything you wish to add or there may be some additional issues you want to raise with us in the first instance?

Mr WILLIAMS - I will 'fess up straightaway: I have been in the job only six weeks but am accompanied by colleagues who have a much deeper knowledge of some of these areas than I. What we have done in the department over the last few years - and I think this audit report relates to 2009-10 - is introduce a number of new systemic approaches to managing and controlling the opportunity for fraud. Two of the biggest ones are mentioned in the response we gave to you. One of them is called 'spend vision', which basically applies an electronic and work-flow transaction approach to credit card bills. Whilst the bits of paper are still to be sighted, there is an electronic mechanism for progressing each itemised credit card bill to an appropriate manager which has to be cleared by the manager using their log-on to log into the system. That gives not only a better accountability for the individual sign-off on the transactions but gives people like the auditors the ability to use those systems to analyse what is going on and where spending is happening. Prior to that, when you just had a paper credit card statement coming in, it was not possible to do that macro analysis of spends and look for trends and spikes and things like that. I am sure Mr Moore and Kane can give you more on that if you would like.

The other thing we have done is try to move as much of the department's administration onto the Finance One system, which you would be familiar with, that gives a standardised set of reporting and ability for people like Kane and the auditors to analyse and spot where things are going wrong. We have also undertaken some education processes, especially out in the broader network where most of our staff are in terms of giving the local business managers instruction sessions on how to deal with financial transactions and things like that.

Quite a lot has happened in those years, probably for very good reason, and we are moving in a better direction than perhaps we were back then. We have not come with any understanding of what areas you might want to delve into. Hopefully we can give you as much as we can today and get what we can't out for you quickly.

Mrs TAYLOR - One of the Auditor-General's concerns was about fraud control planning and review and I see you started to do that somewhere in September 2014. The report was in 2009-10, so why has it taken you that long? Robert, obviously you cannot answer that because you were not there but perhaps somebody else could. If you agreed it needed doing, why has it taken four years to start?

Mr MOORE - The department had a fraud and corruption control plan that was under review. The department implemented Finance One approximately 18 months to two years ago across all schools so we had a major system going in which changed our risk profile. That has an impact on our fraud control risk. That plan was being reviewed at that time by the audit committee and it is up for consideration again now that all those systems are in place.

Mrs TAYLOR - But this is not the first time you have reviewed it since 2010?

Mr MOORE - It is the first that I am aware. I can't answer the question.

Mrs TAYLOR - Is the review you started in September 2014 now complete?

Mr MOORE - Yes, and it is the intention to forward that report to the department's risk management audit committee for sign-off.

Mrs TAYLOR - It is not signed off on yet?

Mr MOORE - Correct.

Ms COURTNEY - Who has responsibility for that report if it is then going to the risk audit committee? Who is responsible for developing this?

Mr SALTER - The responsibility for the policy framework rests with finance. Having said that, we've been working in conjunction with Mat and his team so the overarching policy is what will be submitted to the risk audit committee in late March. It is still in the latter draft stage and not completely finalised, but it will be finalised and should be endorsed at that March meeting. Parallel to that occurring, there has been ongoing internal audit programs on an annual basis where strategic risks are reviewed and an audit plan is approved by the executive in terms of where Mat's focus will be in a particular year. Notwithstanding that the framework has been reviewed, there has been ongoing updates to the annual internal audit plans with a strong element of that being focused on fraud risk.

Mr WILLIAMS - I might add that the methodology has changed over the years since this first report in how we might manage that. As Kane said, while the plan is being review we have not stopped still in what we do in terms of internal audit.

Mr MOORE - In an internal audit, through the auditing standards, we are obliged to be aware of fraud but we don't necessarily go looking for it. We acknowledge that in the development of our internal audit plan. One of the risks we consider in developing our plan is fraud and we have a matrix whereby, in developing our fraud plan, we reconcile that to the department's strategic risks, of which fraud is one of those. It is not an explicit strategic risk but it is a section of one of the strategic risks. Taking that into account in conducting all of our audits we consider the risk of fraud in the context of that audit.

Mrs TAYLOR - The Auditor-General probably takes it a bit more seriously or specifically than that, don't you think? There are a number of areas here in terms of your fraud control planning and fraud prevention and detection where the Auditor-General did not give you a tick, shall we say, in 2010. If he came back now would he give you ticks on these? You don't appear to have done what the Auditor-General has specifically recommended, but there may be other ways you have addressed it that the Auditor-General might accept.

Mr MOORE - I can really only speak from the internal audit perspective. As stated earlier, we do take that into account in developing audit plans. It is not just about detecting fraud but it is about examining explicit actions that business processes and people are taking to mitigate that risk, and it is also about the audit controlled environment that we consider as well. It is an explicit action such as the signing of an invoice or something like that and it is also an educational and broader awareness of fraud risk for staff.

Mr BACON - Broadly when recommendations come down from the Auditor-General to the department, who in the department is responsible to see if they are implemented, or if they are not that there is a reason they are considered and not implemented?

Mrs TAYLOR - What is the process that happens?

Mr WILLIAMS - They would normally go through the internal audit committee.

Mrs TAYLOR - And that's Mat?

Mr WILLIAMS - It is a committee that I think I will now chair.

Mrs TAYLOR - You will chair it rather than an independent chair?

Mr WILLIAMS - It doesn't normally have an independent chair, it normally has an independent member. I chaired the Justice internal audit committee for the last few years and they have an independent member to provide advice.

Mr WATSON - The Auditor-General is a regular attendee at our risk management committee as well.

Mr WILLIAMS - Most of the committees around government, I understand, have the Auditor-General or his representative on them.

Ms FORREST - Is he additional to the independent member?

Mr WILLIAMS - Yes, usually that is the case. I don't think he is a voting member; I think he is there for observation.

Mrs TAYLOR - That is the audit and risk management committee?

Mr WILLIAMS - Yes, internal audit and risk.

CHAIR - On the point Adriana raises about the ticks and crosses, I understand you accepted the crosses the Auditor-General identified in that audit, that there were issues you needed to address, so are you now saying to us that you have addressed all those areas and have a much stronger position moving forward at this time?

Mr WILLIAMS - I think we could probably say we have a stronger position. We haven't finished all of them. The first question Mrs Taylor asked was on point in that we are still working through the final view of the plan. Having said that, we have implemented things such as 'spend vision', which is a major systemic move from a paper-based system to a data-based approach that allows us to analyse and lets auditors have a much greater impact in identifying both opportunities and instances of fraud.

CHAIR - The Auditor-General hasn't followed it up and that is why this committee is following it up, with the AG. This report came out in 2011 and you are telling us that the plan is still being worked through. How many years do you need or want to get that into place?

Mr WILLIAMS - My understanding is that that will come to the internal audit and risk management committee very soon. I believe it is this month.

Mrs TAYLOR - In response to one of the AG's recommendations you said, 'The DOE will investigate the feasibility of amending manager statements of duties to include fraud management'. Has that happened?

Mr WILLIAMS - My understanding is that that is being done as they come up for review.

Mr BACON - So it is included in their statement of duties when they go into the role?

Mr WILLIAMS - Yes. As the duty statement is updated for new people or a change in role, it is being updated to reflect that. We haven't gone back and redone them all.

Mrs TAYLOR - But you are putting that in as part of the statement of duties?

Mr WILLIAMS - Yes.

Mr WATSON - Each time one of the positions come up as vacant and a person applies for the job, they know what they are going into and it includes the new wording.

Ms COURTNEY - I am looking at recommendation 8, that entities should introduce mechanisms to ensure all employees have a general level of fraud awareness. I see what has been done in presentations to school business managers and senior managers in different areas, but do you have any confidence that that is being communicated to all staff? Are there any ways to audit whether you have given that information to all staff and that they have taken it on board? Sometimes the answer might not be within the answer given to us but it might still be occurring within the department somewhere. Just because we don't get the information today doesn't mean it is not occurring, but it is whether or not this recommendation has happened and whether all employees have a general awareness of fraud.

I would have thought there would have to be some kind of mechanism to prove that staff have a general level of awareness, whether it is through some kind of training program, depending on how other policies and procedures are rolled out to all staff.

Mr WILLIAMS - If we can take that on notice, we will come back to you on it.

CHAIR - We will take that on notice and our secretary will write to you with the issues taken on notice.

Ms COURTNEY - I am stepping backwards a bit. We talked about the internal audit and risk committee and then your role as the internal auditor, is that correct? Could you explain to me how the two of those work in terms of does the risk and an audit committee direct your work for the year or give you advice or how does the information flow in hierarchy work between the committee and yourself?

Mr MOORE - Internal audit develops an internal audit plan.

Ms COURTNEY - Is that self-generated?

Mr MOORE - Self-generated and through consultation with senior management and our awareness of risks. When I say develop a plan, I mean we put a plan together and recommend that to the audit committee for consideration.

Ms COURTNEY - Do they generally approve it?

Mr MOORE - Yes, because some of the members of the audit committee are also senior members of the department, so there is a shared understanding as to what the concerns are. Yes, the plan is presented to them, they will consider it, make changes where they believe they are appropriate and then the plan becomes our work plan for that year.

Ms COURTNEY - Who is on the committee as it stands?

Mr MOORE - We have the Deputy Secretary of Department Services; the Director of LINC; myself but I am not a member, I just support the committee; Mark Watson, Director of Industrial Relations and Kane Salter, Director of Finance and Business Services.

Mr SALTER - And the Deputy Secretary, Early Years and Schools.

Ms COURTNEY - And the independent member?

Mr WILLIAMS - There will be but I understand that person has resigned. It is vacant and needs to be filled.

Ms COURTNEY - But it has been filled in the past?

Mr WILLIAMS - Yes.

Ms COURTNEY - For clarity, when this report was released by the Auditor-General, that went through the audit committee at that time?

Mr MOORE - That would be my understanding, from memory.

Ms COURTNEY - Are you satisfied with how the audit committee over the last four or five years has dealt with the recommendations from the Auditor-General?

Mr WILLIAMS - I can't answer that because I have not been there long enough. Have you any observations, Kane?

Mr SALTER - I have only been with the department for 18 months as well. The initial tabling of the report was prior to my time. In seeing the internal audit plans, there has been a good focus on fraud as part of that overall plan because there are other risks that need to be managed, not just fraud. It has been given its due attention in that plan and the audits that have been done.

Ms COURTNEY - I thought it may have fallen off the agenda of the committee and I respect the fact that fraud has been dealt with; I am not asserting fraud has not been looked at but I mean whether or not the specific recommendations have been addressed or whether there has been a turnover in the committee and it has fallen between the cracks.

Mr WILLIAMS - One of the things I discussed with Mat recently was, it does not appear there is a good mechanism at the moment for tracking historical recommendations. I am going to ask the committee when we meet next a couple of things and one of them is, I would like to see a tracking mechanism to see where we are up to. What I have been used to is having a tracking mechanism which also details where the evidence is, that if you are going to put a tick against something, what are you basing it on? It is my intention to introduce that.

CHAIR - To be fair, this committee is looking closely at a number of these issues that the Auditor-General has brought forward, and in due course this committee will be providing a report on it. I notice in answers to a couple of those last questions you said, 'I think,' 'I assume this has happened'; if you need to take that on notice to give us a more specific answer, that might be the better option. I am just saying this is an option open to you about the tracking of the report, where it went to and what happened and so on. This committee would like to know whether or not it was actioned in an appropriate manner.

Mr WILLIAMS - My understanding is that it has been because we have been able to respond to you in relation to what we have done. It is questionable whether some of them have been as timely as they should have been, but my understanding is they have been pursued. If we could take that on notice to find out the mechanism for that and come back to you.

Ms COURTNEY - Thank you.

Ms FORREST - I want to ask a few questions about recommendation 15 regarding corporate cards. I know this has been an issue in the past with the Department of Education and before the Auditor-General's report into fraud. How many cardholders are there at any one school or business unit? Do you have that information?

Mr SALTER - I would have to take that question on notice because it can vary from a small school to a college.

Ms FORREST - I would appreciate it if you could get back to us with that. Can you also say what criteria are used to determine who actually has cards and what the role requires for that facility?

Mr SALTER - The criteria for a card are for all officers who have procurement responsibilities and therefore have a genuine need to have the card. For low-value transactions there is the corporate card. Treasurer's Instructions are that all transactions under $1 000 are to go onto the card so we need to have the cards in the hands of the right people who are undertaking those transactions. Approval for who gets the card in schools would be given by the principal. The principal has to approve the need for a card. In non-school areas, managers/directors would have to approve cards.

CHAIR - The principal of one school could provide a card to a monitor right down the line, whereas another principal might cut it off at a senior teacher, is that what you are saying, or are the principals given guidance as to where it will go?

Mrs TAYLOR - That's why we asked about the criteria.

Mr SALTER - There is guidance again in making sure that the people who have procurement responsibilities and are undertaking a lot of low-value, low-volume transactions can have a card. That can range; traditionally a school business manager would have a card, but there might be some facilities-type people in schools where it also makes sense for the principal to approve the person having a card.

Ms FORREST - The Spendvision program you mentioned earlier tracks all that activity?

Mr SALTER - It tracks all the transactions that are on cards. In schools, except for colleges, principals have to approve transactions on all cardholders' cards, so there is a strong accountability framework there to counter the potential risk with cards. The principal has to approve all of the transactions.

Ms FORREST - A card is linked to a particular person. You cannot say we have the one card, but it will be used by the manager of the cafe who has to buy the bread and milk and the bursar who is purchasing other major items?

Mr WILLIAMS - No, that is one of the specific things you have to sign when you accept the card. There is a whole list of things you can and can't do. For example, you cannot buy fuel on a government credit card, you cannot buy alcohol, you cannot give it to someone else, you have to keep it secure, and those sorts of things. I have come from another department recently where we didn't have Spendvision, so we actually relied on the paper copy of the credit card statement with the receipts attached and that was the only real control. Would it be useful for someone to explain to you what Spendvision actually looks like in terms of how it works?

Mrs RYLAH - Yes please.

Mr WILLIAMS - Kane might be the best person to explain what it looks like in terms of what an employee sees and what a manager sees.

Mr SALTER - For an individual who has a card with transactions offloaded almost daily, the first point would be for the individual to go in and check the transaction was valid and nothing has occurred. They could submit that to the manager for approval then and there and the manager will see that transaction. They might hold off approving it within Spendvision until they have all the transactions for the month and the paper work to support that, but it is visible as soon as the person has said, 'That is a transaction on my card' and submit it through for coding and approval. There is an individual view and a manager view within Spendvision.

Mr BACON - Is there a broader view that looks at the whole system to see if there are any unusual spikes or patterns and things like that behind it?

Mr SALTER - Probably two things. In Mat's internal audit program they do some analysis to see if there are transactions of certain types that could signal issues that need to be looked at. Sometimes there might be valid explanations and other times it might be that a requirement has been broken. In terms of follow-ups on people approving transactions automatic emails come out quite regularly, and they can be annoying, to say that the individual has submitted a transaction through to me for approval and I have not gone into it to approve it yet, so there are automatic follow-ups as well.

Mr BACON - In terms of the government paying its bills on time, is there a facility in there to help people make sure small businesses have their bills paid on time or is it purely for fraud control?

Mr SALTER - Certainly as part of that policy to get small business paid quickly we promoted use of the corporate cards. The Spendvision system can make approval easier and takes away a bit of the barrier for areas to use cards.

Mr BACON - Is there a waiting period then for the manager to tick it off?

Mr WILLIAMS - The card is already charged at that stage.

Mr BACON - So it has gone through and then it is just reviewed?

Mr WILLIAMS - Yes. When Kane uses his credit card I will not approve the electronic transactions on the screen which detail basically what is on the paper transaction until I get the paperwork and the receipts because you need to get a GST receipt or a tax invoice. When I get Kane's credit card statement and he has signed off that it is all okay and work-related, it will have attached the receipts, tax invoices, et cetera. I will then go through and look at them on the screen and check them off, either one by one or you can press 'approval' if they are all going to be approved or you can select the ones you do not approve until you get the evidence you want.

As a manager you look at those transactions and if you see anything unusual you would have not expected someone to have bought or you approved a trip for them and there is a motel booked or whatever, then you get to query and not approve. The system will keep coming back to you in an automated email sense to say you have not approved the transaction for 25 January or for that statement period, so you need to do that. Unless it is approved it stays there as an unapproved transaction.

It is quite a sophisticated mechanism and for people like Mat, instead of having a stack of paperwork to look at he can do analysis systemically so it is a very powerful tool. You can never stop fraud entirely; if people are determined, they will do it.

Mr BACON - How long has it been in place?

Mr SALTER - Approximately 18 months.

CHAIR - It takes me back to when I used to do that and it was a real nightmare to have to go through the invoices and receipts and check them against the credit cards and whether they were permissible or not. Is there no electronic way now in your system to show if somebody has made a purchase for, say, alcohol? Is there is anything in the system that immediately flags that the credit card has been used for alcohol?

Mr SALTER - There is some capability in the system to flag certain merchant types. If there is a transaction against a liquor outlet, it could have a red flag and the manager knows when they look at it that they need to have a closer look at the transaction.

CHAIR - There was talk about that in the Police Service years ago and I was wondering whether it had moved forward.

Mr WILLIAMS - There is some capability but it is still up to the manager to make sure that if a hotel bill comes through they look at the invoice. The first thing I do is check the invoice to make sure no-one has bought alcohol. They can buy their meal but they have to pay for any alcohol with cash out of their pocket.

Ms FORREST - Can you interrogate the information in any way to pick up unusual patterns? I read somewhere that unusual activity on a credit card will often end up with a call from a bank saying, 'Did you make this purchase?', and that is often how they pick up fraud, with people making small claims for things to test out the system. Can you interrogate them that way and look for indications of unusual behaviour?

Mr MOORE - Yes, we can and we do. As part of our internal audit program we have commenced this year a regular review of transactions recorded in Spendvision and Finance One which captures the date of the transaction, the narration, the supplier, the time and those sorts of issues. For example, we use the name of the supplier. If it has the word 'bottle' in it, is that a bottleshop purchase? Sometimes we get noise around that. We are a rather large organisation so there are a number of transactions. We have that capacity and we do it. As Kane mentioned before, though, a lot of our purchases are appropriate in a school environment. If you are doing catering you might need to buy alcohol. That generates quite a bit of a noise for us from an analysis point of view, but we also support that by doing direct testing of the invoices. If we get a sense we can sometimes go from manual paperwork to get a sense whether that noise is just noise or a potential issue.

Ms FORREST - I assume there is a limit on the card - how is that set?

Mr WILLIAMS - That is set by departmental policy and delegations. For example, I have a $1 million spend but a lot of the cards at school level have a lot less than that. There is a graduated spend based on your position. That is by delegation for all financial aspects. I might be signing a contract for $1 million for a building or something like that but my credit card limit is $10 000 a month.

Ms FORREST - When someone is provided with a card, do they get written instructions about the use of it?

Mr WILLIAMS - They do. I have just been through that, having just arrived. I received a package with the card with information about what I can and can't do with it and the bank's information, but I also have to sign a declaration to receive the card, which means that I understand the terms and conditions - no alcohol, no petrol, no giving it away, keeping it secure, et cetera. That is signed and I presume that goes on my personnel file or finance file so that we can come back and say, 'You understood this when you signed it'.

Mrs TAYLOR - You actually checked that the signed thing is returned to you?

Mr WILLIAMS - Whoever is giving out the card is not supposed to give it out unless they get the signed authorisation.

Mrs TAYLOR - Okay.

Mr SALTER - If I could add as well that when you sign in to Spendvision you get a reminder of those responsibilities as well.

Mrs TAYLOR - And at the other end, is returning the card part of the separation or termination? You do not get your final or termination pay until you have returned the card?

Mr WILLIAMS - Certainly that is the practice that I have been used to everywhere else, that your ID cards, your credit card, etcetera, have to go back. We can get some more information on that just to make that absolutely certain.

Mrs TAYLOR - It would be nice to be assured that that in fact happens.

Mr WILLIAMS - I imagine also there are system checks that once you are off the HR system, can your credit card continue or is there any automated process there?

Mr SALTER - You will not have user access to Spendvision anymore and I will have to check about the automatic process of cancelling a card.

Mr WILLIAMS - We will follow that up.

CHAIR - We will take that on notice. With all of this in place with the cards, is it all working? Do you have any cases where cards have been misused and if so, what has happened?

Mr WILLIAMS - Kane, do you have any, without mentioning anything to identify anyone?

Mr SALTER - What we are seeing is good compliance with the policy. Any indiscretions that we might notice are very minor and that has generally been through a lack of understanding. There are a lot of transactions and a lot of purchases, so you would expect -

CHAIR - Not criminal?

Mr SALTER - No, and that hasn't been criminal, it has been -

Ms FORREST - I want to move on to recommendation 16 around internal controls. The Department of Education has established an information security committee that is currently developing an information security plan as required by the Tasmanian Government information security policy manual. I am just wondering what the time frame is for that and how much it has been worked on and is it complete and, if not, when will it be?

Mr WILLIAMS - Can I take that on notice because we do not have the director of IT here who would be responsible for that, and come back to you with the time frame and where it is up to?

Ms FORREST - Okay.

The idea of that was to mitigate fraud risk by developing appropriate risk management strategies. It would be good to have a bit of an update on where that is at, as well as the information security controls that are included in that.

Ms COURTNEY - Ruth, can I just add because I am looking at that one. Recommendation 16 was one of my questions.

Ms FORREST - Can I just keep going with the rest of my question then you can come in? I am just also surprised that Department of Education is going to review its backup processes. I am surprised that that

hasn't already been done. We all would have experienced - most of us anyway - the computer crash that just about destroys your life and with all the education records and stuff I cannot believe that the backup process hasn't been reviewed.

Mrs TAYLOR - This was their response in 2010.

Ms FORREST - I am just interested in the backup process and is it off-site and is it secure, and how is it secure. That may need to be all a part of that question on notice.

Mr WILLIAMS - I will follow that up, I don't have the answer to that. My guess is that this is an old answer and that it will have been reviewed and dealt with probably more than once since then, but let me get the facts for you on notice.

Ms COURTNEY - It seems, from that response, that the information security committee is acting based on the information security plan as stipulated by the Government rather than the recommendation of the Auditor-General. It just so happens that this other recommendation covers some of the Auditor-General's things. It almost goes back to my question previously whether there is a trail of these recommendations having been dealt with through the committee process or through an individual who has now left the department. It is just for us trying to become aware if the process has fallen down, where has it fallen down and why?

Mr WILLIAMS - My guess is, the answer will be that there has been an information security policy in place, being developed through the whole of government that will cover that recommendation and probably more, and that is probably of whole-of-government question to DPAC which has the IT security policy overall. That is what we would be working to add and I am sure that would cover all the recommendations of this audit because it is an overarching plan about computer systems, about security of documents and things like that.

Mrs TAYLOR - That issue here is, that is what is happening now with a whole-of-government plan?

Mr WILLIAMS - Yes.

Mrs TAYLOR - You must have something in place, or have you responded to the Auditor-General's recommendation in the last four years?

Ms COURTNEY - In the last four years, were there any steps taken within the department to address this Auditor-General's recommendation throughout that time?

Mr WILLIAMS - I will have to take that on notice, I do not know.

Mrs TAYLOR - In relation to this question, and it is a question we have asked of all the departments, one of the things we are trying to do is see whether there is a process when the Auditor-General gives out a report, whether or how those recommendations are followed up by any department, and your answers all vary considerably.

Ms COURTNEY - Stepping back to recommendation 14, it talks about once the FCCP is going to be reviewed, which I think is coming up shortly, at that time there is going to be a mechanism for fraud reporting implemented across the department. Do you have a time line for when that might be? It is about the reporting mechanism and it talks about the Integrity Commission's Speak up program, but really getting to the cusp of whether there is a proper internal mechanism for staff reporting allegations and what the time frame will be if that does not exist already.

Mr WATSON - As an agency, we signed up to the Integrity Commission's Speak up program last year and part of that promotion through our staff intranet about the program, also a message from the Secretary about it and also promotion of our grievance procedure. If somebody wants to raise an issue they believe needs to be looked at in terms of the Code of Conduct or an issue that they think is not quite kosher, then there is a process they are directed to as to how they can raise that. That was a fairly heavy promotion of the Speak up program, the message from the Secretary, republishing the grievance procedures and also the mechanism for people to raise issues if they want to.

Mrs TAYLOR - Do you think that got through to the entire staff?

Mr WATSON - It did and went to all staff, bearing in mind -

Mrs TAYLOR - The question is, did it get through to them? Did you just send it out or did you check or did it go through schools or departments?

Mr WATSON - When anything goes out, like a general broadcast to staff, we rely on senior managers to do the follow-up, particularly when it is a message from the Secretary. That is taken very seriously and if the Secretary has made a statement of the message, then managers, as part of their regular meetings and gatherings, would reinforce that. That is what I would do, but I cannot speak for everybody.

Mrs TAYLOR - So you don't check whether that was done? Is there an accounting mechanism?

Mr WILLIAMS - I would need to take that on notice.

Ms FORREST - With regard to recommendation 17 around controls surrounding payment authorisations, I note there was a new financial information management system, Finance One. Has that been successful in addressing the issues raised by the Auditor-General?

Mr SALTER - Prior to Finance One, schools were on individual financial systems. Since coming onto Finance One, they are all in one system; they don't have individual bank accounts anymore or their own cheques. The authorisation through Finance One is along the lines of the school business manager to the principal, so the principal, online, has to authorise all payments. I think that would give good coverage as to what the Auditor-General was highlighting in his recommendation.

Ms FORREST - As to the practical application of this one - for example, I make a financial donation to Hellyer College each year for their scholarship system. With the system now it means that money I donate goes into this system and then, I trust, the money ends up there. How can I be sure that happens?

Mr SALTER - Whilst each school doesn't have its own bank account, it has its own budget centre which clearly distinguishes the funds for that school. If you spoke to the school and asked, 'Can you point to where those funds have gone?', the school would be able to respond to that and know that the overall balance of their budget centre includes that amount.

Ms FORREST - So I could ask Hellyer College to show me that my money went there and they would be able to demonstrate that.

Mr SALTER - Yes.

Mr WILLIAMS - It is like a virtual bank account. They have control over it because they have quite a lot of autonomy over their non-salary funds, but because it is in Finance One it is allocated against certain cost centres. We can see the movement in those, whereas in the past perhaps you couldn't see the movement clearly or follow the transactions from a central point.

Ms FORREST - Going to recommendation 18, which is termination of employees and separation of them, I notice it says, 'Staff requiring their access privilege removed are taken through a quarterly administration process. When an employee separates from DoE or transfers internally access is updated or removed. This should be undertaken quarterly by two senior officers in the payroll area and reviewed by the Manager HR Operations Systems and Recording'. I would have thought quarterly probably wasn't quite enough in view of the fact there is quite a movement of staff at times.

Mr WILLIAMS - I think this is because this is old. You are absolutely right. My understanding is this is now quite an automated process, that when someone is to terminate from the Department of Education, a change made in the HR system which is called the Empower system activates changes to delete the person's access to buildings, IT, all those sorts of things are automated.

One of our answers in a different section at the beginning was that we tightened the credit card control process through the implementation of a termination checklist, so there now is a process to go through so people do not get out the door. All their systems stuff will come off immediately but the credit card is issued by the bank so you have to do something to cancel it.

Mrs TAYLOR - May I raise a practical issue and I am presuming it happens in the Department of Education as it happens in other places. I was talking recently to a person who, in a restructure, has been given a redundancy. This person does not leave the organisation until 1 May but they have already left in actual practice because they have long service leave, et cetera. What would happen in that case? When does the termination happen? Does it not happen until 1 May or does it happen when the person physically leaves and is not going to come back?

Mr WILLIAMS - Technically they will not leave the organisation until the date that their redundancy is effective. If they are not in the organisation because they have taken leave they would largely be treated as an employee on leave until the time of the - the deed has to actually operate. They have to leave and we have to give the money and until then it is only a contingent arrangement.

Mrs TAYLOR - I was thinking that. So what happens to the credit card access, computer access, et cetera, does it remain until the day they actually leave?

Mr WILLIAMS - Certainly in previous areas, largely the person's entitlements, their identification card and building access remain the same unless you have a particular reason to remove them such as they are leaving because there is a disciplinary matter and you have some special concern.

CHAIR - So a person coming in and acting in that role is given another card so you would have two cards operating in that area?

Mr WILLIAMS - They are individually allocated their personal responsibility and liability. If I was to act as a secretary, I would use my card that I have with me, which most senior managers would do. It is not position-specific in one sense, it is a personal liability based on where you are and if you are entitled to a card for your job -

Mrs TAYLOR - It had not occurred to me until we were talking now. In fact that could be a significant risk because there are plenty of people who take forced redundancies, if you like, and there might well be a risk in terms of fraud.

Mr WILLIAMS - They would not be entitled to use their card.

Mrs TAYLOR - They wouldn't?

Mr WILLIAMS - They would not be entitled to use it if they were not at work. If they are on leave they cannot use their card because they are not undertaking work.

CHAIR - Is that a part of the agreement they sign?

Mr WILLIAMS - It is for work-related expenses solely.

CHAIR - On leave they could conduct a work-related expense, they could do that.

Mr SALTER - Where that would get picked up pretty quickly would be my manager seeing a transaction and straight away asking 'What is going on here?' Why is employee *x* using the card? It is not an automatic prevention but I think we would pretty quickly see if there was something happening that should not be.

Ms FORREST - A $10 000 air fare would show up pretty quickly, wouldn't it?

Laughter.

CHAIR - A one-way one would.

Mr WILLIAMS - I think, once again, the thing with fraud is, if someone wants to do it they can do it. It is how quickly your mechanisms pick it up that is the critical issue for us.

Ms FORREST - That is right.

Mr WILLIAMS - I think Spendvision is one of those things that is a fundamental leap in the ability to track credit card transactions and pick up those sorts of things. In paper-based systems there are a lot of time lags in receiving paper statements and things like that.

Ms FORREST - In view of the answers you have given us, I think it would help us if you would all go back and re-read your responses to our questionnaire and send any updated information because clearly some of it is already out of date. We will be writing a report reflecting what you have provided to us as the situation as it is. If it has improved since then I think we need to know. I ask if you could go back - we will have some questions on notice for you - and review all the answers you have provided because I think some of them perhaps do not reflect the reality, from what you have said.

Mr WILLIAMS - I am not sure exactly of the date of these responses.

Ms FORREST - It was 28 November last year.

CHAIR - We have other information to come back to us from today's hearing, but we hope to be in a position in the next month of putting a report in so Ruth's point is a good one.

Ms FORREST - There may not be many areas but for those you have clearly identified as possibly out of date, I think it would be better if they were updated with accurate information for us.

CHAIR - Thank you very much for your attendance here today, Robert and your team, and thank you very much for the way in which you have answered the questions. Again, you are busy people and we understand that. It is important for us to follow up on the Attorney-General's reports and that is what this committee is doing and we will report in due course.

THE WITNESSES WITHDREW.

APPENDIX 3 – REVISED FRAUD CONTROL QUESTIONNAIRES

Questionnaire Special Report No.95 *Fraud Control*

DEPARTMENT OF EDUCATION

Audit criteria 1: Does a suitable management strategy exist?

In assessing the effectiveness of fraud management strategies the Auditor-General paid particular attention to the comprehensiveness of Fraud Control Plans and staff awareness of fraud and fraud control.

The findings for the Department of Education are shown in *Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?*

Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?

Fraud control planning	
Definition of fraud and statement of attitud	✓
Code of Conduct	✓
Fraud control planning and review	×
Fraud Control Officer appointed	✓
Internal audit activity	✓
Fraud prevention and detection	
Fraud awareness	×
Management accountability	×
Fraud risk assessment	✓
Personnel rotation and leave management	✓
Employment screening	×
Mechanisms for reporting suspected fraud	✓

✓ Satisfactory level of compliance
× Recommendations made

Audit criteria 2: Do internal controls prevent and detect fraud?

The Auditor-General also examined the design of the internal control framework and internal compliance with the controls.

The findings for the Department of Education are shown in *Table 2: Findings - Audit Criteria 2 – Do internal controls prevent and detect fraud?*

Table 2: Findings – Audit criteria 2 – Do internal controls prevent and detect fraud?

Findings - adequacy of internal controls	
Cash	✓✓✓
Corporate Card	✓
IT	✓✓
Expenditure and procurement	✓
Payroll	✓✓
Receipts and receivables	✓✓

✓✓✓ Internal Controls were well designed and compliance was satisfactory
✓✓ Internal controls were well designed but compliance needs minor improvement
✓ Either internal control design needs improvement or compliance needs major improvement
× Control design needs major improvement

In accordance with *Audit Act 2008* section 30 the Department was provided a copy of the Report by the Auditor-General, together with a request for comment.

The Department provided the following comments regarding specific recommendations which were included within the Report.

Recommendation #:

#8 – DoE undertakes to increase the general level of fraud awareness amongst its employees through internal communications mechanisms;

#9 – DoE will investigate the feasibility of amending managers' statements of duties to include fraud management;

#11 – DoE will investigate an approach to monitor employees leave balances in high risk positions. However, automatic replacement of staff on leave is not financially feasible;

#12 – All school based positions and a number of non-school positions currently have police checks. DoE will investigate this proposal in relation to other high risk positions;

#14 – DoE has recently communicated to staff the reporting mechanisms available to them and will undertake to continue this practice on a more regular basis;

#15 – DoE has tightened corporate card control processes through the implementation of a termination checklist;

#16 – DoE will investigate the feasibility of developing a security plan and the testing of backups;

#17 – DoE will target improved awareness and compliance with delegated authority and will implement more timely review of exception reports;

#18 – Exception reports are now reviewed and retained. In addition, a termination checklist has been implemented; and

#19 DoE will investigate current revenue reporting framework and consider the best approach to this recommendation.

REPORT RECOMMENDATIONS

The Report made a total of 33 recommendations and the following section of the questionnaire provides each Department the opportunity to demonstrate the actions taken in response to the recommendations of the Auditor-General made for that Department.

Supporting documentation can also be provided as an attachment to your response.

A copy of the Report is attached for the information of the Department.

DEPARTMENTAL RESPONSE TO REPORT RECOMMENDATIONS

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST?

Fraud Control Planning – in *Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?* it is clear that the Department was consistent in its demonstration of a satisfactory level of compliance in the area of fraud control planning. Even so, the following general recommendation does apply to the Department.

Recommendation 4

All entities should review and amend their Fraud Control Plans at appropriate intervals, as a minimum, once every two years

Department of Education response to Recommendation 4:

A review of the Department of Education's (DoE) Fraud and Corruption Control Plan (FCCP) commenced in September 2014. As part of this review, the FCCP will be updated to include a timeframe for formal review which is anticipated to be bi-annually. It is intended to present the revised FCCP to the DoE's Risk Management and Audit Committee in March 2015 for consideration and approval.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST? (CONT.)

Fraud Prevention and Detection – *Table 1: Findings - Audit criteria 1 – Does a suitable fraud management strategy exist?* summarises the fact that a number of recommendations were made in this area for the Department.

Recommendation 8

All entities should introduce mechanisms to ensure that all employees have a general level of fraud awareness that is appropriate for their level of responsibility.

Department of Education response to Recommendation 8:

DoE has increased the general level of fraud awareness amongst its employees through the following:

• 2012 - Presentation at the School Business Managers annual conference by the Manager, Internal Audit Office regarding fraud risks and their management.

• 2013 – Follow up presentation on fraud at the School Business Managers annual conference by the Manager, Internal Audit Office.

• 2014 – Fraud risk management presentation to DoE's Corporate Services Division senior managers by the Manager, Internal Audit Office.

Updates and advice to schools and non-school business units of changes to policy and procedures includes brief commentary, where appropriate, as to how the revised procedure assists in mitigating fraud to maintain an awareness of fraud risks.

As stated in response to Recommendation 9, for all DoE vacancies advertised for SES, Tasmanian State Service Award Band 8 and Band 9, Principals, Assistant Principals and School Business Manager the Statement of Duties are being progressively updated to include responsibility for the management of fraud risks.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST? (CONT.)

Recommendation 9

All entities should ensure that senior managers' statement of duties include fraud management as a required responsibility.

Department of Education response to Recommendation 9:

For all DoE vacancies advertised for SES, Tasmanian State Service Award Band 8 and Band 9, Principals, Assistant Principals and School Business Manager the Statement of Duties are updated to include the following wording in the "Level of Responsibility/Direction and Support" section:

"In the delivery of the Department's activities, the occupant must ensure that:

• Within the occupant's area of organisational responsibility, appropriate strategies are in place to minimise the risk of fraud; and

• Decisions and actions are made ethically and with integrity, on the basis that such is legal, is right and is reasonable based on an objective standard. "

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST? (CONT.)

Recommendation 11

All entities should develop a policy of personnel rotation and ensure that, while employees are on leave, another employee acts in their place.

Department of Education response to Recommendation 11:

DoE monitors employee leave balances. Annually, advice is provided to Principals and managers of employee's whose balances are approaching the upper limits of their award entitlements to assist them in managing leave for these employees and personnel rotation if required.

It is not always financially feasible for DoE to replace staff on leave with another staff member. Backfilling of vacancies resulting from leave is determined on a case-by-case basis and is subject to operational requirements, budgets, the potentially critical nature of the position and the availability of staff. However, when an employee is on leave, their duties are usually distributed to other members of staff as resources permit. This assists in reducing the opportunity for fraud and increases the likelihood of detection.

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST? (CONT.)

Recommendation 12

All entities should perform police checks for senior or high risk positions and document background checks from previous employers.

Department of Education response to Recommendation 12:

Under current DoE policy, all those employed under the Tasmanian State Service Award must obtain a DoE Good Character Check (GCC) prior to commencing employment. The GCC includes a National Criminal History Check. In addition, all applicants for school based positions are required to complete a GCC.

DoE is progressively updating its Statement of Duties (SoD's) to require GCC's be completed for relevant positions. Whenever a vacant position is advertised, the SoD is reviewed and if necessary, based on the nature of the position and after appropriate approval, the following is inserted in the *Requirements* section as an essential requirement...

"The Head of the State Service has determined that the person nominated for this office is to satisfy a pre-employment check before taking up the appointment, promotion or transfer"

DoE's *Selection Process Guidelines* recommends that selection panels consider a range of verification processes that includes seeking referee reports and contacting people other than cited referees. The GCC process supports this by seeking written permission from the applicant "for the Department of Education to check (my) previous volunteer or employment history, if deemed necessary"

AUDIT CRITERIA 1 – DOES A SUITABLE FRAUD MANAGEMENT STRATEGY EXIST? (CONT.)

Recommendation 14

All entities should communicate their formalised reporting mechanisms to staff more effectively.

Department of Education response to Recommendation 14:

The DoE is participating in the Integrity Commission's Speak-up program. This program is currently promoted on the homepage of the DoE's intranet, accessible to all DoE staff. The aim of the program is to help identify and eradicate misconduct (which includes the misuse of resources). Staff are referred to DoE's grievance resolution process, DoE's Conduct and Investigation Unit, the Integrity Commission and the Ombudsman.

Further, on completion of the review of the FCCP, it is intended that the FCCP will be broadly circulated to promote fraud awareness and to provide details of DoE's fraud reporting mechanisms.

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD?

In *Table 2: Findings – Audit criteria 2 – Do internal controls prevent and detect fraud?* a number of control areas within the Department were identified as in need of improvement and the following recommendations were made in the context of the audit findings.

Recommendation 15

DoE should improve corporate card controls by tightening relevant administrative processes.

Department of Education response to Recommendation 15:

The DoE has implemented an IT system (Spendvision) that has improved the control, monitoring and administration of corporate card expenditure. Corporate card usage can now be centrally monitored to support supervisors and managers in controlling the extent and use of corporate cards.

In relation to the specific observations made in the report, managers now receive independent advice through Spendvision of corporate card transactions that have been allocated to their school or business unit that require approval. Managers can now also independently review corporate cards issued to their school or business unit, assisting in the identification of corporate cards to be cancelled due to staff separations. Also, the cardholder is not required to obtain a replacement card when internally transferred, reducing the risk that a cardholder may be in possession of two active cards.

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD? (CONT.)

Recommendation 16

DoE should develop and implement:

- an IT security plan that covers all aspects of the IT environment, particularly those aspects that relate to fraud prevention and detection;

- a regular schedule for testing.

Department of Education response to Recommendation 16:

DoE has established an Information Security Committee that is currently developing an Information Security Plan as required by the Tasmanian Government Information Security Policy Manual. Implementation of the Information Security Plan will assist in mitigating fraud risk by:

• Developing appropriate risk management strategies.

• Direct the preparation, review and approval of the agency's information security policy framework.

• Ensure that the implementation of information security controls is coordinated across the agency.

• Review and approve methodologies and processes for information security.

• Assign responsibility for and oversee the management of information security registers.

The DoE will also review its backup processes and procedures to cover the information assets in the Information Security Plan.

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD? (CONT.)

Recommendation 17

DoE should:

- tighten controls surrounding payment authorisation;

- ensure that all exception reports produced are properly reviewed and that an appropriate audit trail exists in the expenditure and procurement areas.

Department of Education response to Recommendation 17:

A new financial information and management system, Finance1, was implemented in schools in 2012/13. This is the same system used by the non-school sector of DoE. All payments can now only be made by the electronic authorisation of two, independent people. Who can approve payments is managed by the logical access controls of Finance 1.There is further segregation in the payment process in that although schools and business units have the ability to approve the payment, the finalisation of the payment and transfer of funds to the supplier can only be processed by the DoE's centralised accounts payable staff.

Finance 1 also provides a strong audit trail. It captures details of the payment as well as by whom and when the transaction was entered, approved, posted and paid to the supplier.

In relation to the observation made in the audit report regarding creditor creation exception reports, independent reviews of all creditor creations within Finance 1 are now completed on a weekly basis.

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD? (CONT.)

Recommendation 18

DoE should:

- ensure that all exception reports produced are properly reviewed and retained in the payroll area; and

- develop a termination checklist to ensure employees' access privileges are removed.

Department of Education response to Recommendation 18:

DoE has developed a fortnightly certification process to ensure that payroll area staff are checking payroll exception reports that are returned to the payroll area by schools or business units. There are automated mechanisms within this certification process to alert senior payroll staff when schools or business units fail to certify fortnightly payroll information. This process enables payroll staff to follow up directly with the school or business unit the required certification.

Staff requiring their access privileges to be removed are detected through a quarterly administration process. When an employee separates from DoE or transfers internally, access is either updated or removed. This review is undertaken quarterly by two senior officers of the payroll area and reviewed by the Manager, HR Operations, Systems and Reporting.

AUDIT CRITERIA 2 – DO INTERNAL CONTROLS PREVENT AND DETECT FRAUD? (CONT.)

Recommendation 19

DoE should compare actual cash receipts to budgeted cash flow in all areas so that variances are promptly identified and investigated appropriately.

Department of Education response to Recommendation 19:

The introduction of Finance 1 across all areas of DoE (school and non-schools) has allowed all business units of the DoE to run ad hoc or periodic reports that can be utilised to monitor actual to budgeted cash flows or against proportionate budgeted cash receipts.

Monthly reports are provided to DoE's executive group detailing the budget performance of school and non-school based business units. A soon to be released on-line financial reporting system available to relevant staff within schools and business units also incorporates reporting on key aspects of financial management.

Appendix 2 -

The following have been updated from the information we initially provided in response to the Questionnaire to provide further information:

Recommendation 9: reworded to show changes have been implemented

Department of Health and Human Services response to Recommendation 9:

DHHS have implemented changes to the wording contained in its Statements of Duties to communicate its position on fraud and to inform workers (including senior managers) of the obligations and responsibilities they have in relation to fraud prevention and management.

The Statement of Duties template were updated in 2014 and changes will be made to current Statements of Duties as they are reviewed from January 2015.

Recommendation 21 - Steve from OCIO has put together some additional words around how the password policy addresses fraud specifically.

Department of Health and Human Services response to Recommendation 21:

A standard password policy controls network logon password complexity, basic access permissions, and expiry criteria. The use of the DHHS "Active Directory" infrastructure by key and critical systems (e.g. Patient Administration System) as an authentication service provides a consistent framework for authentication and access control. The Finance One system uses an additional internal security mechanism, consisting of an independent security domain, for access to the system. Investigations into the use of the 'Fine Grained Password Policy' feature enabled during a recent upgrade will allow OCIO to enforce stricter password policies on user network accounts. This will allow Business areas to nominate users or roles, where the risk of fraud due to network logon misuse is high, and stronger passwords are required.

As part of its obligations to the Tasmanian Government, OCIO undertakes risk assessments of all new Internet facing systems where the risk of fraud due to the unauthorised use of logon credentials is identified. Security assessments of Internet facing systems by independent experts include the use of the 'Open Web Application Security Project' (OWASP) standards which include recommendations for minimum password strength and complexity.

OCIO is currently trialling the Networking Tasmania Two Factor Authentication service as a further measure for securing remote access to sensitive systems, which will significantly reduce the likelihood of network accounts by external attackers.

The default workstation configuration on all DHHS computers locks the screen after 10 minutes of inactivity. This can however be varied by OCIO where it would adversely impact business processes.

The "Commvault" backup infrastructure used to protect all DHHS server infrastructure automatically tests backup sets when moving data between storage pools on a regular schedule. Additionally the ability to recover data from backup is tested on a regular basis as (in addition to Disaster Recovery) it is used to recover data lost through human error. The Finance System is backed up every week night. The most recent system recovery process was undertaken on 3 September 2014 and involved the complete recovery of the system to an alternative non-production environment.

Housing Tasmania system support officers (SSOs) perform quarterly or ad hoc checks for duplicates. While the SSOs have access to two accounts (one single admin account and an individual account each), no individual has two or more logon accounts to their name. The administrator password is also changed on a

fortnightly basis. This report is then compared against THIS users and relevant users are deactivated in THIS and Centrelink is contacted to deactivate that user's Single Point Enquiry access. Additionally, the SSOs also respond to requests from the Service Centres to deactivate users.

All network logon accounts are issued to staff via formally managed processes. This is predominantly done by the automated creation of accounts based on staff being 'on boarded' by Human Resources via the Payrolls system, or by forms countersigned by an appropriate manager and actioned via the OCIO IT Service Centre. Where staff cease employment with the Department or THOs their account is automatically disabled. This covers permanent staff, part time staff, and contractors and locums employed by the Department, Service Groups (e.g. Housing Tasmania and Ambulance Tasmania) as well as the three Tasmanian Health Organisations (which includes the Launceston General Hospital).

Wherever possible staff are required to use their personally issued network logon and password to access IT systems. There are some circumstances where this is not practical (e.g. shared ward computers) and business practices require the use of shared logons.

Access to the Ambulance Tasmania Computer Room is controlled by a separate dedicated security system under the direct control of Ambulance Tasmania. Access to this room is only permitted where it has been explicitly authorised by an appropriate Ambulance Tasmania Officer. Access for maintenance works must be booked in advance and authorised by an appropriate Ambulance Tasmania Officer. Access is controlled using individually issued access cards.

Recommendation 22 - In relation to creditor changes, I have detailed what the current practice is

Department of Health and Human Services response to Recommendation 22:

Internal Audit undertook a review on creation and amendment of creditor accounts in 2011. Testing found that for the majority of creditor creations and amendments, appropriate documentation was on file that had been completed by authorised officers and entered into Finance One by approved users. Some entries were found that did not have documentation to back them up. Further investigation indicated that this was due to the request forms attached to emails sent to Finance being saved incorrectly for a number of files. Recommendations were made.

Since 2011, all creditor creations and amendments and supporting documentation are now stored electronically on the central drive in Finance Operations.

The recommendation to improve controls within Housing Tasmania re invoice authorisation is sourced from audit sample testing as part of this review. Two invoices from a much larger sample were found to have not been authorised appropriately. Whilst this represents a relatively low error rate, the management of Housing Tasmania recognises the importance of process controls in this area and have sought to strengthen internal controls accordingly. Subsequent financial audits of Housing Tasmania have undertaken similar testing and have not disclosed any identified errors.

The Launceston General Hospital (LGH) as a part of the Tasmanian Health Organisation – North (THO-N) has a process for proper documentation to be generated and retained for all orders which are generated. Given the number of areas undertaking ordering from a variety of systems, electronic ordering for all orders isn't practical.

As an example when undertaking manual orders, the initial request is completed via a blue non-stock requisition form. This form is then approved by a delegated officer and goes to the appropriate area where an electronic request is then completed based on the details that are included in the original request.

The process is controlled with there being a limited number of people with the delegation to approve the original blue non-stock requisition forms and also limited people with the access to raise the resulting electronic requisition requests.

No issues have been raised via internal or external audits since 2011 with regards to the order processes within THO-N.

The recommendation to review system processes at Ambulance Tasmania to ensure that initiation and authorisation are independent relates to the finding that purchase orders raised by an employee could be referred to their spouse (another employee) for authorisation. The controls within Ambulance Tasmania's purchasing system ensure that there is always a separation of duties between the raiser of a purchase order and the approver. Wherever possible, a familial relationship between the employee who raises the purchase order and the approver is avoided. If this situation cannot be avoided to ensure timely operations processes exist for the transaction, approval is reviewed by a third party.