2011

PARLIAMENT OF TASMANIA

AUDITOR-GENERAL SPECIAL REPORT No.95

Fraud control

February 2011

Presented to both Houses of Parliament in accordance with the provisions of Audit Act 2008

Printed by:

Print Applied Technology, Hobart

© Crown in Right of the State of Tasmania February 2011

Auditor-General's reports are available from the Tasmanian Audit Office, HOBART, although in limited supply. This report and the recent titles shown at the back of this report can be accessed via the Office's home page. For further information please contact:

Tasmanian Audit Office

GPO Box 851

Hobart

TASMANIA 7001

Phone: (03) 6226 0100, Fax (03) 6226 0199

Email: admin@audit.tas.gov.au

Home Page: http://www.audit.tas.gov.au

This report is printed on recycled paper.

ISBN 978-0-9808688-3-8

1 February 2011

President
Legislative Council
HOBART

Speaker
House of Assembly
HOBART

Dear Madam President
Dear Mr Speaker

SPECIAL REPORT NO. 95
Fraud control

This report has been prepared consequent to examinations conducted under section 23 of the *Audit Act 2008*. The objective of the audit was to assess the effectiveness of fraud management strategies in selected State entities.

Yours sincerely

H M Blake
AUDITOR-GENERAL

Contents

List of Tables

Foreword

This performance audit was conducted in the context that the incidence of fraud is increasing in Australia as is the average financial loss associated with fraudulent conduct. The Introduction to this Report quotes one reference indicating that the total cost of fraud to the Australian community was $8.5bn while another study noted the total value of fraud reported was $301.1m.

However, quantifying the actual level of fraud is difficult because some frauds are either undetected or go unreported. Also, the nature of frauds is changing as is the complexity of the business environment in which we operate. Importantly, fraudulent behaviour does not only result in loss of assets but can result in significant additional direct and indirect costs suggesting that investment in cost effective systems aimed at minimising and detecting fraud is not only worthwhile, but essential.

Recently the Tasmanian public sector has identified five reported fraudulent incidents suggesting we are not immune to fraudulent behaviour. This performance audit identified a range of improvements that need to be made by State entities to manage the risk of fraud with the responses to recommendations made received positively.

H M Blake

Auditor-General

1 February 2011

List of acronyms and abbreviations

AT	Ambulance Tasmania (part of DHHS)
DHHS	Department of Health and Human Services
DoE	Department of Education
EFT	Electronic funds transfer
HT	Housing Tasmania (part of DHHS)
IT	Information technology
LGH	Launceston General Hospital (part of DHHS)
TFS	Tasmania Fire Service
THIS	Tasmanian Housing Information System
UTAS	University of Tasmania

Executive summary

Executive summary

Background

The incidence of fraud within the Australian economy is increasing, as is the average financial loss associated with fraudulent conduct. In 2007, the Australian Institute of Criminology estimated that the total cost of fraud to the Australian community was $8.5bn. More recently, the total value of fraud reported in KPMG's 2008 fraud survey was $301.1m, with an average value of $1.5m for each organisation.

The integration of fraud into the overall risk management is therefore essential. Fraud management and response plans, codes of conduct and governance codes are some of the policies that assist in raising employee awareness. Issuing a policy by itself however is insufficient. People need to be educated and held accountable to these guidelines or behaviours are unlikely to change.

Entities should also ensure that all business processes, particularly those assessed as having a high exposure to fraud, are subject to a rigorous system of internal controls that are well documented, updated regularly and understood by all personnel.

An effective internal control system is not protection against fraud. However, it is obvious that such a system is a vital element of an appropriate fraud control program. Reasonable controls along with internal audit testing, improve the likelihood that fraud indicators will be detected and considered for further investigation.

Audit conclusion

Creating the right culture

During the course of the audit, we noted common findings in the areas of:

- general fraud awareness
- employment screening
- fraud reporting mechanisms
- personnel rotation policies
- fraud risk assessment
- management accountability.

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.

Internal controls

Cash controls were robust at DoE and DHHS, however deficiencies were found in other areas tested.

Service Tasmania was highly rated in all areas except for expenditure, procurement and particularly IT where deficiencies were found with system access controls.

The control framework at TFS needs strengthening, with major deficiencies in areas of cash, corporate cards, IT, expenditure and procurement.

The control framework at UTAS was robust for the majority of areas tested, with payroll and receipts rated highly. However, deficiencies were noted in the areas of cash, IT, expenditure and procurement.

Of the various systems tested, we noted that IT controls needed improvement in all entities.

List of recommendations

The following table reproduces the recommendations contained in the body of this Report.

Rec No	Section	We recommend that …
1	1.2.1	… TFS and *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 ▪ communicate the fraud definition and statement of attitude to fraud to all employees.
2	1.2.2	… UTAS should develop a Code of Conduct that defines expected behaviour for all employees.
3	1.2.3	… TFS and *Service* Tasmania should develop comprehensive Fraud Control Plans that address specific fraud risks relevant to them.
4	1.2.3	… all entities should review and amend their Fraud Control Plans at appropriate intervals, as a minimum, once every two years.
5	1.2.3	… UTAS should promptly implement internal audit's recommendations.
6	1.2.4	… TFS and *Service* Tasmania should consider assigning the role of Fraud Control Officer to manage their exposure to this risk.

Rec No	Section	We recommend that …
7	1.2.5	… TFS should revise its decision to not have an internal audit function.
8	1.3.1	… 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	1.3.2	… all entities should ensure that senior managers' statements of duties include fraud management as a required responsibility.
10	1.3.3	… TFS, LGH, AT, HT and *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.
11	1.3.4	… all entities should develop a policy of personnel rotation and ensure that, while employees are on leave, another employee acts in their place.
12	1.3.5	… all entities should perform police checks for senior or high-risk positions and document background checks from previous employers.
13	1.3.6	… TFS should develop an alternative reporting mechanism and communicate this mechanism to staff, via a Fraud Control Plan.
14	1.3.6	… all entities should communicate their formalised reporting mechanisms to staff more effectively.
15	2.3.2	… DoE should improve corporate card controls by tightening relevant administrative processes.
16	2.3.3	… 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	2.3.4	… 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.

Rec No	Section	We recommend that …
18	2.3.5	… 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.
19	2.3.6	… DoE should compare actual cash receipts to budgeted cash flow in all areas so that variances are promptly identified and investigated appropriately.
20	2.4.2	… 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	2.4.3	… 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.

Rec No	Section	We recommend that …
22	2.4.4	… 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	2.4.5	… 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	2.4.6	… LGH should ensure that there is appropriate segregation of duties.
25	2.5.2	… 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	2.5.3	… *Service* Tasmania should ensure that an appropriate audit trail exists to support information provided in monthly budget variance reports.
27	2.6.2	… TFS should: ▪ ensure that all bank reconciliations are properly reviewed ▪ improve the strength of electronic fund transfer (EFT) controls.
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.

Rec No	Section	We recommend that …
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.
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.
31	2.7.2	… UTAS should improve system design to better assist in the performance of bank reconciliations.
32	2.7.3	… UTAS should: ▪ develop a password policy that considers current best practice ▪ ensure that computers automatically lock when left unattended.
33	2.7.4	… UTAS should review changes to the creditor master file on a regular basis and ensure that an appropriate audit trail exists.

This page left blank intentionally

Audit Act 2008 section 30 — Submissions and comments received

Audit Act 2008 section 30 — Submissions and comments received

Introduction

In accordance with section 30(2) of the *Audit Act 2008*, a copy of this Report, together with a request for comment, was provided to the following State entities selected for this audit:

- Department of Health and Human Services
- Department of Education
- Department of Primary Industries, Parks, Water and Environment
- Tasmania Fire Service
- University of Tasmania.

Similarly, a summary of findings along with a request for comment or submissions was also provided to the Treasurer and the Ministers for:

- Health
- Human Services
- Education and Skills
- Police and Emergency Management
- Primary Industries and Water
- Environment, Parks and Heritage.

The comments and submissions provided are not subject to the audit nor the evidentiary standards required in reaching an audit conclusion. Responsibility for the accuracy, fairness and balance of those comments rests solely with those who provided a response or comment.

Submissions and comments received

Department of Education

Recommendation 8

DoE undertakes to increase the general level of fraud awareness amongst its employees through internal communication mechanisms.

Recommendation 9

DoE will investigate the feasibility of amending managers' statements of duties to include fraud management.

Recommendation 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.

Recommendation 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.

Recommendation 14

DoE has recently communicated to staff the reporting mechanism available to them and will undertake to continue this practice on a more regular basis.

Recommendation 15

DoE has tightened corporate card control processes through the implementation of a termination checklist.

Recommendation 16

DoE will investigate the feasibility of developing a security plan and the testing of backups.

Recommendation 17

DoE will target improved awareness of and compliance with delegated authority and will implement more timely reviews of exception reports.

Recommendation 18

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

Recommendation 19

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

Department of Health and Human Services

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.

Department of Primary Industries, Parks, Water and Environment (*Service* Tasmania)

The comments below are made in relation to both *Service* Tasmania and more broadly the Department of Primary Industries, Parks, Water and Environment (DPIPWE).

Firstly, Management notes that the report has 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 improvements 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 e.g. 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 the 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.

Tasmania Fire Service

Recommendation 1

TFS has recently developed a set of values 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.

Recommendation 3

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.

Recommendation 4

Once developed TFS will review its Fraud Control Plan bi-annually.

Recommendation 6

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.

Recommendation 7

TFS considers its size limits the resources available to have a specialist internal audit role or a fraud control role.

Recommendation 8

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.

Recommendation 9

TFS will consider introducing into its senior managers' statement of duties fraud management responsibilities.

Recommendation 10

TFS will review its current risk register particularly in relation to fraud.

Recommendation 11

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.

Recommendation 12

TFS will introduce police checks for senior or high-risk positions.

Recommendation 13

TFS considers there is a clear reporting mechanism for ethical breaches in the organisation and that this has been clearly explained to all staff.

Recommendation 14

This has been done in internal courses delivered by Human Services.

Recommendation 27

Processes have been implemented to provide monthly reporting on major reconciliations.

EFT controls are considered reasonable.

Recommendation 28

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 required to be completed prior to finalisation of terminating pay. This is to include certification of the return of corporate cards and other TFS property.

Recommendation 29

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. 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.

Recommendation 30

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 were not evidenced.

University of Tasmania

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
- 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.

This page left blank intentionally

Introduction

Introduction

Background

The Commonwealth's Fraud Control Guidelines (the Guidelines) define fraud as 'dishonestly obtaining a benefit by deception or other means'[1]. The 'benefit' referred to in this definition does not have to be tangible and, according to the Guidelines, can include the following types of offences:

- theft
- obtaining a financial advantage or any other benefit by deception
- causing a loss, or avoiding or creating a liability, by deception
- making, using or possessing forged or falsified documents
- unlawful use of computers, vehicles, telephones and other property or services.

Within the Australian economy, the incidence of fraud is increasing as is the average financial loss associated with fraudulent conduct. In 2007, the Australian Institute of Criminology estimated that the total cost of fraud to the Australian community was $8.5bn. More recently, the total value of fraud reported in KPMG's biennial fraud survey was $301.1m, with an average value of $1.5m for each organisation[2].

There are a number of obvious direct costs associated with fraud such as lost outputs associated with the time taken in dealing with detected frauds, business disruptions while 'fraud-proofing' computer systems and replacing staff dismissed for fraud. Indirect costs also exist such as decreased employee morale with its attendant impacts on productivity, estimated to be at least one-third of the direct costs[3].

Quantifying the actual level of fraud is difficult because some frauds are either undetected or go unreported. Additionally, the nature of fraud is changing as commercial practices evolve and entities adopt new approaches to service delivery and make greater use of e-commerce.

Because of its pervasive nature, the integration of fraud risk into the overall risk management frameworks is essential. Some of the means

[1] Commonwealth Fraud Control Guidelines — May 2002, http://www.ag.gov.au/, accessed 22 November 2010.

[2] KPMG Fraud Survey 2008, http:/www.kpmg.com.au/aci/docs/FraudSurvey2008a.pdf, accessed 22 November 2010.

[3] Counting the Costs of Crime, http:/www.aic.gov.au/documents/B/F/D/%7BBFD22E46-3E66-431A-B74D-F76661CCB103%7Dtbp004.pdf, accessed 22 November 2010.

that assist in raising employee awareness are fraud management and response plans, codes of conduct and governance codes. However, issuing a policy by itself is an inadequate response; people need to be made aware and made accountable otherwise attitudes — and behaviours — are unlikely to change.

The Tasmanian public sector experience

The Tasmanian public sector is not immune to the increasing rate of reported fraudulent incidents with some recent examples being:

- Cradle Mountain Water — an accounts officer defrauded the authority to the tune of $1.2m between 2006 and 2009. The money was spent on mortgage payments, holidays, furniture, computers and eBay purchases.
- Ambulance Tasmania — a former executive, in charge of daily financial management, defrauded the Service of $650 000 over eight-and-a-half years. Offences included forgery and obtaining goods by false pretences.
- Tasmania Fire Service — a finance clerk, who had been a trusted employee for 10 years, was convicted of defrauding more than $370 000 in October 2003.
- Tasmanian Association for Mental Health — a former executive officer transferred almost $280 000 from the employer's account into a personal account and forged cheques. The money was spent on holidays, clothes and mortgage payments.
- The Office of the Director of Public Prosecutions — a former Tasmanian Crown Prosecutor stole more than $200 000 from the Tasmania Police property store between 2003 and 2007 to fund a gambling addiction.

Models of better practice

During the course of the audit, we explored models of better practice that address fraud risk management for the public sector. The risk of fraud is not new in either the public or private sector and, as a result, there is a growing body of literature in relation to both the rising occurrence of fraud and the latest fraud management strategies.

Although the nature of public and private sector business is inherently different, we found that the most comprehensive guidelines applied to the private sector only, namely the Australian standard AS 8001-2008 *Fraud and Corruption Control*. So, we used its fraud control framework as our better practice model.

In addition, Commonwealth Fraud Control Guidelines have existed since May 2002 and provide valuable guidance for departments when developing fraud risk management strategies.

Both sets of guidelines provide direction in defining fraud, effective fraud control principles as well as relevant roles and responsibilities.

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.

The following clients 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
- Tasmania Fire Service (TFS)
- University of Tasmania (UTAS).

Audit criteria

The audit criteria that we developed for this audit were aimed at addressing effectiveness aspects as follows:

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

Format of the report

In Chapter 1, we use a holistic approach to examine the effectiveness of fraud control strategies. Particular attention is paid to the comprehensiveness of Fraud Control Plans and staff awareness of fraud and fraud control.

Chapter 2 examines both the design of the internal control framework and internal compliance at each individual entity with comments on the results.

Audit approach

To conduct the audit, we:

- reviewed fraud-related documentation
- interviewed relevant staff
- conducted employee surveys
- tested internal control compliance
- evaluated the overall control environment.

In some cases, we used the work of internal and external auditors.

Timing

Audit planning commenced in December 2009. Fieldwork was completed in January 2010 with reporting finalised in December 2010.

Resources

The total cost of the audit was $147 000.

This page left blank intentionally

1 Do anti-fraud cultures exist?

1 Do anti-fraud cultures exist?

1.1 Background

AS 8001-2008 *Fraud and Corruption Control* and the Commonwealth Fraud Control Guidelines make it clear that organisational culture is an essential element in managing fraud risk. Specifically, fraud control is a holistic concept involving the implementation and continuous monitoring of fraud prevention, detection and response mechanisms.

To signal its commitment to a sound ethical culture, there are a number of things that an entity can do. A vital step is to establish an integrity framework that contains a code of conduct, a process of benchmarking and continuous monitoring, underpinned by senior management that sets an example for other employees. Fraud management and response plans are examples of policies that assist in raising fraud awareness in employees.

A Fraud Control Plan documents an entity's intended action in implementing and monitoring the entity's fraud prevention and response initiatives. The Plan should be integrated with an overall risk management plan.

Effective implementation of the fraud control strategy relies on making employees accountable. Regular communication is necessary to ensure management and employees are informed of fraud control issues, including current best practice. Through those communications, the Fraud Control Plan needs to be accessible to all staff, particularly those with specific fraud control accountabilities.

A fraud control strategy also involves the appointment of a Fraud Control Officer, whose primary responsibility is to manage the entity's exposure to fraud risks. The Fraud Control Officer would have the capacity to understand and translate current best practice in fraud and corruption control into user-friendly practices and procedures, as well as the ability to deliver and coordinate training, particularly to line management.

1.2 Planning for fraud control

Proper planning and coordinated resourcing are key elements in any anti-fraud program. Table 1 provides a summary of the findings in this area.

Table 1: Findings — planning for an anti-fraud culture

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

1.2.1 Definition of fraud

The regular dissemination of the fraud definition should be accompanied by an explicit statement that fraudulent practices within the entity will not be tolerated. This excerpt from the UTAS Control of Fraud and Corruption policy provides an example of an unequivocal statement towards fraud:

> UTAS has zero tolerance of fraud and corruption. Fraudulent or corrupt activity of any kind, including for the benefit of UTAS, will not be tolerated. All staff and students must, at all times, conduct themselves in a manner consistent with the law and UTAS rules regulations and policies.

During the course of the audit, we noted that two clients, TFS and *Service* Tasmania had not yet adopted a fraud definition or communicated a statement of the entity's attitude to fraud to all employees.

Recommendation 1

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

1.2.2 Code of Conduct

A code of conduct is an important element of a sound integrity framework because it clarifies for employees what is and what is not

acceptable within the organisation. The definition of fraud should be aligned with a comprehensive code of conduct which sets out the entity's expected standards of behaviour. An example is the requirement of the State Service Code of Conduct that 'an employee must use Tasmanian Government resources in a proper manner'.

As the *State Service Act 2000* applies to all entities in scope, with the exception of UTAS, the State Service Code of Conduct is relevant. Consequently, we found that UTAS was the only client whose organisation had not implemented a Code of Conduct that defined expected behaviour for all employees. While significant effort had been made to identify expected behaviour for students and academics, the same effort had not been applied to defining acceptable behaviour for support staff.

Recommendation 2

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

1.2.3 Fraud control plan

A fraud control plan outlines the entity's intended actions in implementing and monitoring fraud and corruption prevention, detection and response initiatives. To be effective, a fraud control plan should be reviewed and amended at intervals appropriate to the entity.

We found varying progress in the development, implementation and review of Fraud Control Plans.

- UTAS had developed a fraud control strategy in 2007, subsequently reviewed by internal audit in 2009. Recommendations from that review had not been implemented at the time of audit.
- DHHS had implemented a comprehensive fraud control strategy in 2009.
- DoE had only recently finalised a fraud control policy that had been in draft form for the previous four years.
- *Service* Tasmania and TFS had not developed a fraud control plan.

Recommendation 3

TFS and *Service* Tasmania should develop comprehensive Fraud Control Plans that address specific fraud risks relevant to them.

Recommendation 4

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

Recommendation 5

UTAS should promptly implement internal audit's recommendations.

1.2.4 Fraud Control Officer appointed

Though not necessarily a full-time role, a Fraud Control Officer contributes to the entity's fraud risk and mitigation strategies. This is achieved by translating current best practice into user-friendly practices and procedures, as well as delivering training on relevant procedures, particularly to line management.

During the audit, we found that only two clients, TFS and Service Tasmania had not assigned the role of Fraud Control Officer.

Recommendation 6

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

1.2.5 Internal audit activity

Although primary responsibility for the identification of fraud and corruption within an entity rests with management, internal audit activity can be an effective part of the overall control environment to identify indicators of fraud.

During the course of the audit, we noted that TFS did not have an internal audit function. This meant that there was no program for the review and amendment of internal controls and no program that assessed compliance with internal controls.

Recommendation 7

TFS should revise its decision to not have an internal audit function.

1.3 Creating the right culture to prevent and detect fraud

The following table summarises those controls designed to create the right culture to prevent and detect fraud.

Table 2: Findings — creating the right culture to prevent and detect fraud

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

1.3.1 Fraud awareness

The most likely way for internal fraud to be detected is by observation, investigation and reporting by colleagues of the perpetrator(s)[4]. Ideally, all employees need to have a general awareness of fraud, including the appropriate response if this type of activity is detected or suspected.

To determine the level of fraud awareness at each entity, we used a fraud awareness survey instrument[5]. We asked a random selection of employees a series of questions about their understanding of fraud, their entity's activities in raising fraud awareness and their possible response to detected fraud.

From our survey, we found that:

- There is no ongoing training in the use of the Code of Conduct and Fraud Control Plan for decision-making.
- Most employees felt that they had not received sufficient fraud awareness training suitable for their level of responsibility.
- Employees felt that more training and discussion around changes in fraud-related policies and procedures, and the Code of Conduct, was required.

[4] AS 8001-2008: *Fraud and Corruption Control*

[5] The survey instrument is reproduced in the Appendix.

In some cases, employees were unaware of the Fraud Control Plan and the reasons that they undertook internal control activities.

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.

1.3.2 Management accountability

Management accountability requires senior management to have a general understanding of fraud, including knowledge of:

- the prevalence of fraud in Australia
- types of fraud common within the operating environment
- robustness of the entity's internal control environment
- knowledge of frauds that have been detected in the entity in the last five years
- knowledge of new technology tools for detecting and preventing fraudulent activity.

Organisations can ensure that managers have that awareness by listing the responsibilities in statements of duties. Awareness can be further strengthened by incorporating fraud management into employees' performance management systems.

We found that none of the audited entities had incorporated fraud risk management into their statements of duties or their performance management systems.

Recommendation 9

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

1.3.3 Fraud risk assessment

Entities should adopt a process which allows for the systematic identification, analysis and evaluation of fraud risk and should periodically conduct a comprehensive assessment of the risks of fraud. Typically, this assessment should be performed at least every two years and be conducted in accordance with AS/NZS ISO 31000:2009 *Risk management — Principles and guidelines*.

During the course of the audit we found that risk registers at TFS, LGH, HT, AT and Service Tasmania did not address the risk of fraud.

Recommendation 10

TFS, LGH, AT, HT and *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.

1.3.4 Personnel rotation and leave management

Fraudsters often carry out and conceal their activities by not going on leave and allowing anyone else to do their jobs. Therefore, it is prudent for entities to have a policy of personnel rotation to minimise situations of single person dependency. This can be achieved by encouraging employees to take leave and rotating personnel through positions that may be more susceptible to the risk of fraud. For example, positions in which the employee has access to the entity's funds or confidential information will be more susceptible to fraud than other positions.

We found that a policy of personnel rotation did not exist in any of the entities tested. Evidence for this was twofold: all entities had some employees with leave balances that were above the reasonable limit; and, when an employee did go on leave, it was not always the case that someone would act in their position. There is a statutory maximum leave balance that applies to all individuals employed under the *Tasmanian State Service Award* and is the equivalent of two years' accumulated leave credits. A similar limit has been enforced at TFS through the *Tasmanian Fire Fighting Industry Employees Award*. Although the statutory maximum leave balance does not apply to UTAS and some DHHS employees, for the purposes of the audit, the statutory requirement was viewed as a reasonable limit.

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.

1.3.5 Employment screening

Many employees who have committed workplace fraud have a history of dishonest conduct with previous employers[6]. Agency exposure can be limited by employment screening processes such as employment history checks and police checks[7]. Employment screening should be considered for all new employees joining the

[6] The KPMG Fraud Survey 2006 that found that 14 percent of employees involved in fraudulent conduct within the entity had a prior history of dishonest conduct with a previous employer compared with seven per cent in the 2004 survey. http://www.kpmg.com.au/aci/docs/FraudSurvey2008a.pdf.

[7] Public Sector Agencies are entitled to conduct police checks for crimes of dishonesty provided they obtain approval from the Commissioner pursuant to section 18(1)(l) of the *State Service Act 2000*. When advertising a position Agencies need to state in the position advertisement that a pre-employment check will be conducted. Refer to Commissioner's Direction No. 10/2001.

entity (including contractors) and all personnel being moved into a senior or a high risk position in terms of the potential exposure to fraud.

During the course of the audit, we found that there was a general lack of consistency across organisations in relation to employment screening. We noted that:

- Only *Service* Tasmania undertook police checks for all employees. HT, LGH and UTAS did not perform police checks and TFS only performed police checks on career and volunteer fire-fighters.
- With the exception of DHHS units, our brief review of all other audit clients' recent recruitment files provided no evidence of background checks from previous employers.

Recommendation 12

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

1.3.6 Mechanisms for reporting suspected fraud

Fraud prevention and detection is enhanced where entities have alternative effective mechanisms for employees to report suspicious or known illegal or unethical conduct. Examples of possible mechanisms are reporting through the Fraud Control Officer, Human Resources Manager or Finance Manager. The existence of those mechanisms needs to be widely known by employees and demonstrably supported.

We noted that the only reporting option for TFS employees was via direct managers. A consequence is that an employee would have no effective reporting mechanism if concerned about the conduct of their own supervisor. We also found that although the other entities had formalised alternative reporting pathways, employees were unaware of those pathways.

Recommendation 13

TFS should develop an alternative reporting mechanism and communicate this mechanism to staff, via a Fraud Control Plan.

Recommendation 14

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

1.4 Conclusion

During the course of the audit, we noted common weaknesses in the areas of:

- general fraud awareness
- employment screening
- fraud reporting mechanisms
- personnel rotation policies
- fraud risk assessment
- management accountability.

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

2 Do internal controls prevent and detect fraud?

2 Do internal controls prevent and detect fraud?

2.1 Background

Effective internal controls are not a complete defence against fraud, but such systems are a vital element of an appropriate fraud control program. Further, control systems should include elements of prevention and detection and be well documented, updated regularly and understood by all personnel.

In this Chapter, the risk of fraud being perpetrated in the areas of cash, corporate cards, Information Technology (IT), expenditure, procurement, receipts, receivables and payroll is considered. Examples of fraudulent acts in these areas include:

- Cash — an employee steals money from the entity's bank account.
- Corporate card — an employee makes purchases that are for their own personal benefit.
- Expenditure and procurement — an employee creates a fictitious company and lists the bank account as his or her own, invoices are then sent to the entity and authorised by said employee for payment.
- Receipts and receivables — while collecting money for goods supplied, an employee sells an individual item, fails to write an invoice and collects the payment and deposits the money into a personal bank account.
- Payroll — an employee creates a fictitious employee ('ghost') and lists the bank account for salary payment as his or her own and the employee is paid via the fortnightly payment run.

This Chapter investigates the appropriateness of the internal control framework and examines whether the entities in scope took reasonable steps to alleviate the risk of fraud.

2.2 Summary of internal control findings

Table 3 provides a summary of the control strength in each area tested. Individual ratings from the Table are reproduced throughout Chapter 2.

Table 3: Findings — adequacy of internal controls

Control Area	DoE	DHHS	TFS	ST	UTAS
Cash	✓✓✓	✓✓✓	✓	✓✓✓	✓
Corporate card	✓	✓✓	✓	✓✓✓	✓✓✓
IT	✓✓	✓	✓	✓[8]	✓✓
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.

2.3 Department of Education

The Department of Education (DoE) provides services through: Early Years; Learning Services and Schools; Information Services and Community Learning; and Skills Tasmania. These services are delivered through 209 schools and colleges, nine Learning and Information Network Centres, 46 public libraries, 60 online access centres and five Adult and Community Education Centres around Tasmania. DoE is also responsible for the operation and management of the Tasmanian Archive and Heritage Office, State Reference Service and Parliamentary Library.

A consequence of the geographical distribution of DoE's operations is an increased risk of fraud. Australian standard AS 8001-2008 *Fraud and Corruption Control* identifies that fraud often occurs in operations that are geographically remote from the entity's central management. This is because local operations are often not subject to adequate levels of corporate scrutiny and local management may not see the

[8] This rating is made in respect of Department of Primary Industries, Parks, Water and Environment as the provider of *Service* Tasmania's IT services.

need for fraud control measures or, in some cases, compliance with these measures. Other relevant risk factors were:

- volume of transactions
- extent to which technology is involved in the transactions
- previous incidence of fraud within the general economy.

2.3.1 Cash controls

We found that cash controls were robust and made no adverse findings.

Rating: ✓✓✓

2.3.2 Corporate card controls

Monthly corporate card statements were reconciled on a timely basis and the duties were appropriately segregated between the purchasing officer and authorising officer. However, we were concerned that:

- Approximately three per cent of cards belonged to people who were no longer employees.
- Around one per cent of cards belonged to employees who had transferred to another school and had subsequently been issued another card even though a new card was not required. This resulted in a number of employees possessing two active cards.

Rating: ✓

Recommendation 15

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

2.3.3 IT controls

We noted that DoE did not have an IT security plan. On the other hand, there was a well integrated permissions system, reinforced by unique user IDs, appropriate physical security of servers and time-out locks.Although back-ups were performed, they were not tested in a live environment. This created a risk that audit-log evidence may not be available in the event of a fraud. Rating: ✓✓

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 backups.**

2.3.4 Expenditure and procurement controls

Recent changes had been introduced to improve fraud control including a register of personal and pecuniary interests. A register of this kind supports an ethical culture by ensuring greater transparency of employee conduct. We also found that DoE had standard authorisation controls, although unlike other users of the standard public sector finance system, electronic delegation limits had not been enforced.

A number of weaknesses were identified in relation to DoE's payment and procurement controls. Our view, during the course of the audit, was that no payment should be possible without the signatures or electronic authorisation of two people with awareness of the details of the payment. We found two instances where the purchasing and authorising officers were the same person. Two instances were also noted where an employee had authorised payments in excess of their financial delegation.

We also found that a report detailing changes to the creditor master file could be generated by the system for any selected period. At the time of this audit, however, there was no evidence that this report was routinely generated or reviewed.

Rating: ✓

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.**

2.3.5 Payroll controls

DoE payroll controls in place at the time of audit were satisfactory. Timesheets were authorised appropriately, employee leave entitlements were current and all employees tested were genuine employees.

We noted however, that there were two former employees who still had payroll system permissions but did not have general logon rights to enable access to the payroll system. Also, two out of the three exception reports viewed had not been reviewed.

Rating: ✓✓

Recommendation 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.**

2.3.6 Receipts and receivables controls

The design of the current receipts and receivables control framework was reasonable, with regular reconciliations and reviews of outstanding debts. However, we noted one Head Office area in which actual cash receipts were not compared to budgeted cash flows. This means that any unexpected decrease in revenue could not be promptly identified and investigated appropriately.

Rating: ✓✓

Recommendation 19

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

2.4 Department of Health and Human Services

The Department of Health and Human Services (DHHS) is responsible for delivering integrated services that maintain and improve the health and wellbeing of Tasmanians. DHHS entities that were included in this audit were Housing Tasmania (HT), Launceston General Hospital (LGH) and Ambulance Tasmania (AT).

- HT provides a range of housing assistance for eligible low-income Tasmanians or those who have special housing needs. The main risk factor identified at HT included the geographical distribution of operations.
- LGH is a 300-bed public hospital serving the north of Tasmania. The main risks identified were the existence of portable and attractive assets and a high volume of transactions.
- AT provides emergency ambulance care, rescue and transport services and a non-emergency patient transport service through a network of 45 urban, rural and remote ambulance stations. The main risk factors identified at AT included the geographical distribution of operations and the previous fraud at AT (see the Introduction).

Some of the functions at DHHS are delivered at a corporate level, such as payroll and IT. Other functions are performed at a business

unit level with examples being expenditure and procurement. Where there are findings that relate to the business unit, these are discussed in subsections below.

2.4.1 Cash controls

Cash controls were robust and we made no adverse findings.

Rating: ✓✓✓

2.4.2 Corporate card controls

The DHHS Finance (Finance) unit controls the administration of corporate cards at all DHHS entities, but the responsibility of managing corporate cards is shared between Finance and the individual entities.

Without exception, we found that expenditure was business-related. We also noted that reconciliations were performed and segregation of duties was appropriate. However, some control discrepancies were noted:

- At HT, one card reconciliation statement was not available, one transaction had not been authorised and three cards had not been retrieved from separating employees.
- At LGH, there was one instance where transaction documentation could not be located.

Rating: ✓✓

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

2.4.3 IT controls

IT is managed centrally by the DHHS Information Technology unit. This unit is responsible for developing IT-related policies, maintaining security, providing maintenance and development of IT systems for the entities included under the DHHS umbrella. As a result, the IT control framework was predominantly tested at the DHHS level.

The majority of employees had unique user IDs and passwords, there were suitable restrictions placed on access to systems and the physical security of servers was predominantly adequate.

Weaknesses included the lack of a finance system security policy, non-enforcement of time-out settings for computer sessions and network security settings not meeting some password complexity standards. We also noted that although back-ups were performed, they were not tested in a live environment. This created a risk that audit-log evidence may not be available in the event of a fraud.

In relation to the Tasmanian Housing Information System (THIS), we found:

- A number of employees had two user IDs to access the system.
- Six former employees still had THIS system permissions but did not have general logon rights to enable access to the THIS system.
- There was a lack of procedures for updating system access following staff transfers and terminations.

At LGH, there were a number of users with system access that could not be verified as current employees.

At AT, employees working in the Communications room did not have unique user IDs and passwords. A similar problem existed with server room access which was controlled by a common key.

Rating: ✓

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 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.**

2.4.4 Expenditure and procurement controls

Responsibility for expenditure and procurement is shared between the DHHS Financial and Business Performance unit (DHHS Finance) and individual business units. As a general rule, purchase

requisitions, orders and deliveries occur at the business unit, while invoices are matched at DHHS Finance.

During the audit, we found that creditor changes were reviewed. However, we were concerned that following the departure of an employee, there was a lack of evidence of that review prior to April 2010. We were advised that Internal Audit intended to investigate this matter.

At HT, we noted that there were two physical invoices that bore no evidence of authorisation or costing details.

At LGH, we were unable to perform audit testing in relation to supporting documentation and original invoice control despite repeated requests for access to systems or documentation. Despite this, we identified the following discrepancies:

- Some orders were not performed by the central purchasing unit and, as a consequence, the finance system did not record order details such as requisitioning officer.
- Four delegates could approve higher limits than they could actually initiate.

At AT, we noted that a process was built into the system where the purchase orders raised by an employee could be referred to their spouse (another employee) for authorisation. During the testing however, there were no instances found where this actually occurred.

Rating: ✓

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 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 system processes at AT to ensure that initiation and authorisation are independent.**

2.4.5 Payroll controls

The Pay and Personnel Unit at DHHS is a centralised unit servicing all DHHS entities. As a result, we tested payroll controls at the DHHS level.

The current payroll control framework at DHHS was robust. There was limited access to payroll records, leave entitlements were kept current and, in most cases, timesheets were appropriately approved.

Discrepancies noted included:

- classification changes to the payroll database not checked by an independent officer
- two instances where the Pay and Personnel Unit was unable to produce quality assurance reports
- one instance where the pay report was prepared and printed, but had not been approved.

Rating: ✓✓

Recommendation 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.**

2.4.6 Receipts and receivables controls

The receipts and receivables functions are generally performed by individual DHHS entities and performance in this area is brought together at the DHHS level to provide high-level information to the Departmental Executive.

We found that outstanding debts were appropriately reviewed, that segregation of duties was satisfactory at HT and AT and the information provided at the Departmental Executive level was adequate.

However, we noted that segregation of duties at LGH was weak in that a number of employees who were able to raise invoices could also initiate credit notes and process receipts.

Rating: ✓✓

Recommendation 24

LGH should ensure that there is appropriate segregation of duties.

2.5 Service *Tasmania*

Service Tasmania provides one-stop access for government transactions, services and information. These services are provided via phone and internet and also through 27 shops located around Tasmania. Operational management for *Service* Tasmania's three service delivery channels is provided through its 'lead agencies' — Telecommunications Management Division in the Department of Premier and Cabinet, DoE and Department of Primary Industries, Parks, Water and Environment, which is the lead agency for shop services. Our audit activity concentrated on shop services.

Risk factors indentified included the high volume of transactions, extensive use of technology and substantial cash flows.

2.5.1 Cash, corporate cards, payroll and receipts controls

We found that controls for all of the above areas were robust and made no adverse findings.

Rating: ✓✓✓

2.5.2 IT controls

There were adequate IT security policies in place, access to information systems was suitably restricted and the physical security of servers and back-ups were deemed appropriate. However, we found that user accounts were not always terminated on a timely basis and the network security settings did not meet password complexity standards.

Rating: ✓

Recommendation 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.**

2.5.3 Expenditure and procurement controls

Service Tasmania's expenditure and procurement control framework was robust. Compared to other entities, *Service* Tasmania employees raise a small number of purchases and as a result, this area is one where the risk of fraud has been minimised. However, we found that while budget variances were regularly investigated, documentation to support this activity could not be provided.

Rating: ✓✓

Recommendation 26

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

2.6 Tasmania Fire Service

The Tasmania Fire Service (TFS) is the operational arm of the State Fire Commission and includes over 230 fire brigades across Tasmania. The main risk factor identified was the geographical distribution of TFS operations.

2.6.1 Payroll and receipts controls

We found that payroll and receipts controls were robust and made no adverse findings.

Rating: ✓✓✓

2.6.2 Cash controls

There was adequate segregation of duties and other cash controls were in place. However, we noted that only 44 per cent of bank reconciliations tested had been properly reviewed and that there were weak controls surrounding internet banking[9].

Rating: ✓

Recommendation 27

TFS should:

- **ensure that all bank reconciliations are properly reviewed**
- **improve the strength of electronic fund transfer (EFT) controls.**

2.6.3 Corporate card controls

The corporate card control framework was robust, with timely reconciliation of monthly corporate card statements. However, we found that segregation of duty controls were not always adhered to with one transaction being raised and approved by the same employee. We also noted two active cards belonging to former employees who had left TFS in 2009.

Rating: ✓

[9] Specific details of existing weaknesses have been provided to TFS in a management letter.

Recommendation 28

TFS should ensure:

- **compliance with the segregation of duty control in the corporate card area**
- **cancellation of corporate cards for terminating employees.**

2.6.4 IT controls

The IT control environment at TFS was robust, with adequate IT security policies in place, unique user IDs and passwords and an automatic time-out of computer sessions.

However, we noted that passwords were only required to be reset every twelve months, which did not meet best practice requirements. Although back-ups were performed, we found they were not tested in a live environment. This created a risk that audit-log evidence may not be available in the event of a fraud. Furthermore, we noted that the server room was accessed by a shared key available to a select group of employees.

Rating: ✓

Recommendation 29

TFS should:

- **develop a password policy that considers current best practice**
- **improve server room access controls**
- **develop a regular schedule to test backups.**

2.6.5 Expenditure and procurement controls

At TFS, we found standard authorisation controls. However, a number of deficiencies were noted including:

- three transactions that were not in accordance with financial delegations
- inadequate segregation of duties in that employees could perform cheque and EFT runs as well as invoice entry
- a financial delegations register that did not reflect current position titles
- a lack of evidence that creditor changes were reviewed.

Rating: ✓

Recommendation 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.**

2.7 University of Tasmania

The University of Tasmania (UTAS) is an international university operating out of Tasmania. Its three major campuses are the Sandy Bay, Newnham and Cradle Coast, while there are also two study centres in New South Wales. Additionally, UTAS units are offered in China, Malaysia and Kuwait.

The main risks identified were the geographical distribution of operations, high volume of transactions, availability of portable and attractive assets and the extent to which technology is involved in the transactions.

2.7.1 Corporate cards, payroll and receipts controls

We found that controls for all of the above areas were robust and made no adverse findings.

Rating: ✓✓✓

2.7.2 Cash controls

A new finance system was implemented prior to the commencement of audit fieldwork. Due to the new system implementation, we noted that there were some problems around auto-matching receipts which resulted in a number of unreconciled items.

Rating: ✓

Recommendation 31

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

2.7.3 IT controls

At UTAS, access to records was suitably restricted, physical security of computers was maintained at all times, an overarching IT security policy existed and back-ups were tested at regular intervals.

However, network security settings did not meet password complexity standards and time-out of staff computer sessions was not enforced although the default setting was set for time-out.

Rating: ✓✓

Recommendation 32

UTAS should:

- **develop a password policy that considers current best practice**
- **ensure that computers automatically lock when left unattended.**

2.7.4 Expenditure and procurement controls

The payment and procurement control framework at UTAS was robust, with appropriate exception reporting, budget control and requirements for new supplier creation. However, we noted that there was no evidence of regular review of creditor changes.

Rating: ✓✓

Recommendation 33

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

2.8 Conclusion

Cash controls were robust at DoE and DHHS, however deficiencies were found in other areas tested.

Service Tasmania was highly rated in all areas except for expenditure, procurement and particularly IT where deficiencies were found with system access controls.

The control framework at TFS needs strengthening, with deficiencies in areas of cash, corporate cards, IT, expenditure and procurement.

The control framework at UTAS was robust for the majority of areas tested, with payroll and receipts rated highly. However, deficiencies were noted in the areas of cash, IT, expenditure and procurement.

Of the various systems tested, we noted that IT controls needed improvement in all entities.

This page left blank intentionally

Independent auditor's conclusion

Independent auditor's conclusion

This independent conclusion is addressed to the President of the Legislative Council and to the Speaker of the House of Assembly. It relates to my performance audit of fraud control in selected State entities, namely.

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

At each of those entities, I reviewed documentation, interviewed relevant staff, conducted surveys with a sample of employees, undertook testing of internal control compliance and evaluated the overall control environment. In undertaking the audit, I used the work of internal and external auditors in some cases. My audit was based on the objective, scope and audit criteria detailed in the Introduction to this Report (see page 14).

In developing the scope of this audit and completing my work, the audit clients provided me with all of the information that I requested. There was no effort by any party to the audit to limit the scope of my work. This Report is a public document and its use is not restricted in any way by me or by any other person or party.

Responsibility of the Heads of Agencies, or equivalents, of the State entities selected for audit

The Heads of Agencies, or equivalents, of the State entities are responsible for establishing and maintaining ethical cultures within their entities that manage fraud risk. Also, they are responsible for designing, implementing and maintaining systems that prevent and detect fraud.

Auditor-General's responsibility

In the context of this performance audit, my responsibility was to express a conclusion on whether or not the State entities selected for audit adequately managed the risk of fraud within their respective entities.

I conducted my audit in accordance with Australian Auditing Standard ASAE 3500 *Performance engagements*, which required me to comply with relevant ethical requirements relating to audit engagements. I planned and performed the audit to obtain reasonable

assurance whether the State entities adequately managed the risk of fraud within their respective entities.

My work involved obtaining evidence of management support in developing and maintaining anti-fraud organisation cultures. Additionally, I undertook sample testing of system controls in a range of business processes aimed at preventing and detecting fraud.

I believe that the evidence I have obtained was sufficient and appropriate to provide a basis for my conclusion.

Auditor-General's conclusion

Based on the audit objective and scope and for reasons outlined in the remainder of this Report, 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.

Cash controls were robust at DoE and DHHS, however deficiencies were found in other areas tested.

Service Tasmania was highly rated in all areas except for expenditure, procurement and particularly IT where deficiencies were found with system access controls.

The control framework at TFS needs strengthening, with deficiencies in areas of cash, corporate cards, IT, expenditure and procurement.

The control framework at UTAS was robust for the majority of areas tested, with payroll and receipts rated highly. However, deficiencies were noted in the areas of cash, IT, expenditure and procurement.

Of the various systems tested, we noted that IT controls needed improvement in all five entities.

H M Blake

Auditor-General

1 February 2011

This page left blank intentionally

Recent reports

Recent reports

Tabled		Special Report No.	Title
Oct	2007	69	Public building security
Nov	2007	70	Procurement in government departments
			Payment of accounts by government departments
Nov	2007	71	Property in police possession
			Control of assets: Portable and attractive items
Apr	2008	72	Public sector performance information
Jun	2008	73	Timeliness in the Magistrates Court
Jun	2008	74	Follow up of performance audits April–October 2005
Sep	2008	75	Executive termination payments
Nov	2008	76	Complaint handling in local government
Nov	2008	77	Food safety: safe as eggs?
Mar	2009	78	Management of threatened species
May	2009	79	Follow up of performance audits April–August 2006
May	2009	80	Hydro hedges
Jun	2009	81	Contract management
Aug	2009	82	Head of Agency contract renewal
Oct	2009	83	Communications by Government and The Tasmanian Brand project
Oct	2009	84	Funding the Tasmanian Education Foundation
Nov	2009	85	Speed-detection devices
Nov	2009	86	Major works procurement: Nation Building projects, Treasurer's Instructions 1299 and 1214
Jun	2010	87	Employment of staff to support MPs
Jun	2010	88	Public Trustee — management of deceased estates
Jun	2010	89	Post-Year 10 enrolments
Jul	2010	90	Science education in public high schools
Sep	2010	91	Follow of special reports: 62–65 and 70
Oct	2010	92	Public sector productivity: a ten-year comparison
Nov	2010	93	Investigations 2004–2010
Nov	2010	94	Election promise: five per cent price cap on electricity prices

Current projects

Current projects

Performance and compliance audits that the Auditor-General is currently conducting:

Title	Subject
Profitability, and economic benefits to Tasmania, of Forestry Tasmania	Evaluates Forestry Tasmania's long-term financial and economic performance.
Follow up of special reports	Ascertains the extent to which recommendations from Special Reports 69–73 (tabled from October 2007 to June 2008) have been implemented.
Fire management	Examines whether respective government entities have implemented the recommendations from the COAG 2004 report titled *National inquiry on bushfire mitigation and management*.
Tourism Tasmania — Value for money?	Examines the effectiveness of Tourism Tasmania with respect to: promotions and advertisements; websites and implementation of planned strategies and initiatives.
Out-of-home care	Assesses the effectiveness of some aspects of the efficiency of out-of-home care as an element of child protection.
Urban Renewal and Heritage Fund and Premier's Sundry Grants Fund	Assesses the expenditure incurred on the Urban Renewal and Heritage Fund and the Premier's Sundry Grants Fund in recent years and compliance with the approved protocols and budgets.

Appendix

Appendix

Fraud awareness survey instrument

Reproduced here is the survey instrument referred to in Section 1.3.1 of this Report.

No	Question
1	What types of activity constitute fraudulent or corrupt practices?
2	What do you believe are the biggest risk factors risk factors in relation to fraud and corruption?
3	How would you respond if you detected or suspected fraudulent or corrupt activity?
4	How would you report allegations or concerns regarding fraud or unethical conduct?
5	What measures does your entity take to raise staff awareness of fraud control?
6	Does training include new types of technology that may be used for the commission of fraud and technological measures that can be used by your entity to minimise new types of fraud?
7	Do you feel that you receive regular fraud awareness training that is appropriate to your level of responsibility?
8	How are updates and changes to fraud-related policies, policies, procedures, the Code of Conduct and other ethical pronouncements communicated to employees? Do you feel that this is effective?
9	Do you sign an annual statement to the effect that you have over the previous 12 months, complied with the entity's Code of Conduct and fraud and corruption policies and that you will comply over the next 12 months?
10	Are you aware of the internal controls that are operational within your entity?
11	Are you able to access documentation relating to your entity's internal controls?
12	Why do you feel it is important to adhere to your entity's internal controls?
13	If you suspected a colleague was committing a fraudulent act would you report it?
14	Do you feel confident that there will be no negative consequences of reporting the suspected fraudulent activity?