Review of the States of Guernsey's anti-fraud governance framework

Private and Confidential

16 April 2013

Ernst & Young LLP

ERNST & YOUNG

Ernst & Young LLP
PO Box 9, Royal chambers
St. Julians Avenue
St. Peter Port
Guernsey GY1 2AF
Tel: 01481 717400
Fax: 01481 713901
www.ey.com/channel_islands

Private and confidential

Deputy Heidi J. R. Soulsby, Chairman
Public Accounts Committee
States of Guernsey
Sir Charles Frossard House
PO Box 43, La Charroterie
St Peter Port
Guernsey
GY1 1FH

16 April 2013

Ref: DRJM/SdF

Direct Line: 01534 288697

Email:dmoore@uk.ey.com

Dear Deputy Soulsby

Review of the States of Guernsey's anti-fraud governance framework

We are pleased to attach our report in respect of the above matter.

Scope of our work

In accordance with your instructions, we have performed the professional services set out in our engagement letter dated 30 October 2012. The scope of these services is attached as Appendix A of this report.

As a result, we have produced a findings and recommendations report on:

a) The appropriateness[1] of the States of Guernsey's anti-fraud governance framework pre May 2012;

b) The reasonableness of the recommendations and actions set out in the internal audit reports issued in May 2012 and August 2012;

c) The appropriateness[2] of the States of Guernsey's anti-fraud governance framework subsequent to these recommendations and actions; and

d) Our recommended next steps, prioritised through discussion with you.

We completed our fieldwork on 17 December 2012.

For the avoidance of doubt, it should be noted that the scope of this report does not include the investigation of the July 2012 alleged mandate fraud incident.

[1] We note that the States of Guernsey does not have a defined risk management framework and communicated risk appetite. Therefore our approach to the review of the anti-fraud governance framework will be performed utilising our expectations of an organisation of equivalent size and complexity.

[2] ibid

Limitations on execution of scope of our work

All documentation and information used was provided by you, the States of Guernsey or interviewees. We have not sought to obtain further information or to corroborate information provided to us.

On 4 December 2012 the Public Accounts Committee ("PAC") wrote to the former Chief Officer of the Treasury & Resources Department to invite him to meet with us for the purposes of this report. On 17 December 2012 the PAC received a response, stating he had already provided a comprehensive statement in relation to this matter and was not aware of any additional evidence he could usefully add.

Deputy Lyndon Trott was identified as an additional interviewee, in agreement with the PAC. However Deputy Trott was unable to meet with us prior to the finalisation of our fieldwork. The PAC wrote to Deputy Trott and, as an alternative, provided him with the opportunity to raise any points against the scope of this stage of the review by letter by 7 January 2013. No such letter was received from Deputy Trott.

Variation in the scope of our work

The Treasury & Resources Principal Assistant was identified as an interviewee by the PAC in our engagement letter. However he is new to role and it was subsequently agreed with the PAC that it would not be relevant to meet with him for the purposes of this report and to vary our scope accordingly.

Work performed

We performed the scope of services attached as Appendix A and, as a result, we:

- Were provided with and analysed the documents listed in Appendix B.
- Conducted interviews with the individuals listed in Appendix C.

Our work has been limited to the scope detailed in our engagement letter as agreed with you and we stress that more detailed procedures may reveal issues that this engagement has not. This Report is based on the sources and types of information set out above. We have not sought to confirm the accuracy of the information provided to us.

The receipt of further information may cause us to qualify or amend the findings reported herein. If, for any reason, we subsequently consider that the report requires further qualification or amendment, we will notify you.

Because our procedures did not constitute either an audit or review made in accordance with International Standards on Auditing or International Standards on Review Engagements, we did not intend, or seek, to express any opinion on the information. Our procedures did not constitute an audit and should not be relied on as such.

Where we have made assumptions during the course of our work, we have explained these assumptions within this report.

Limitations of use and distribution of the report

This report was prepared on your specific instructions solely for the purpose of this engagement and should not be relied upon for any other purpose. It should not be quoted referred to without our prior consent in writing. We assume no responsibility whatsoever in respect of or arising out of or in connection with the contents of this report to any other parties. If others choose to rely in any way on the contents of this report they do so entirely at their own risk.

Structure of the report

Section 1 is our executive summary. Section 2 is an overview of an anti-fraud governance framework. Section 3 is explains the Ernst & Young anti-fraud maturity model and details our summary assessment of the States' anti-fraud maturity. Sections 4 to 6 set out our findings by reference to the scope of our work. Section 7 details our recommended next steps, prioritised through discussion with you.

We appreciate the assistance of both the PAC and the interviewees in carrying out our work and look forward to providing any further assistance if so requested.

We shall be pleased to discuss the findings set out in this report with you. If you have any queries regarding our findings please do not hesitate to contact me or Samantha des Forges.

Yours sincerely

David Moore
Partner
Ernst & Young LLP

Abbreviations

Abbreviation	Definition
States	States of Guernsey
PAC	Public Accounts Committee
T&R	Treasury and Resources Department
AFGF	Anti-fraud Governance Framework
IAU	Internal Audit Unit
NAO	National Audit Office
2000 Report	States Audit Commission: Report on risk management and insurance, 2000
2006 Report	National Audit Office: Risk Management and Insurance in the States of Guernsey, March 2006
WAO Report	Welsh Audit Office: Review of Good Governance – The States of Guernsey, dated 4 September 2009
April 2012 Report	PAC: Review of Risk Management and Insurance, April 2012
Fraud Guideline	Administrative and Accounting Guideline: Fraud and Other Irregularities
Fraud Rule	States of Guernsey Rules For Financial and Resource Management Finance Rules: Fraud

Contents

1. Executive summary

Overview

1.1 In July 2012 it was reported that the States had suffered an alleged mandate fraud to the value of £2.6m.

1.2 Whilst the financial and management time impact of this fraud cannot be underestimated, it can also be viewed as a catalyst to drive through change and a more corporate approach to risk management generally, and anti-fraud in particular.

1.3 The "climate is right" to ensure that there is a robust and fully embedded anti-fraud governance framework across the States. Anti-fraud must be owned by staff at all levels, but the change must be driven by the right "tone from the top".

Findings

1.4 Our principal findings, which are explained more fully in the subsequent sections of this report, may be summarised as follows:

- The States' anti-fraud governance framework pre May 2012 was inappropriate compared to an organisation of similar size and complexity.
- The recommendations and actions set out in the internal audit reports issued in May 2012 and August 2012 are not unreasonable.
- Although not tested, we believe that, as at the completion date of our fieldwork (17 December 2012) the States' anti-fraud governance framework has been improved and the Head of Internal Audit[3] has played a pivotal role in driving forward the October 2012 States' Fraud Risk Management Improvement Plan, which has resulted in much of this improvement.
- However, as at 17 December 2012, the States' anti-fraud governance framework is still inappropriate compared to an organisation of similar size and complexity. This is due to a number of factors, including:
  - That some planned actions are dependent on the identification of a corporate fraud lead;
  - That some planned actions are dependent on the new SAP system ("the Hub") going live on 1 January 2013; and
  - Other competing priorities, such as the Financial Transformation Programme.
- Subsequent to the successful completion and embedding of the further planned actions detailed in the October 2012 States' Fraud Risk Management Improvement Plan, the States' anti-fraud governance framework would be expected to move further towards a position of 'established/advanced'.
- To meet our 'baseline expectation' as set out in the Ernst & Young anti-fraud maturity model, the States' anti-fraud governance framework would still require additional actions before being deemed appropriate compared to an organisation of similar size and complexity.

[3] On 1 November 2012 the Head of Internal Audit became the States Head of Assurance

2. An anti-fraud governance framework

2.1 This section describes the objective of an anti-fraud governance framework and our approach to the review. It establishes our baseline expectations of an anti-fraud governance framework in an organisation of equivalent size and complexity to the States.

Objective of an anti-fraud governance framework

2.2 The objective of a robust anti-fraud governance framework is to contribute to an organisation achieving its strategic objectives through effective fraud risk management. Effective fraud risk management aims to support the achievement of the following:

- Development and maintenance of an anti-fraud culture;
- Deterring fraud against the organisation (increasing the 'perception of detection') and preventing external fraud attempts;
- Detection and investigating fraud incidents; and
- Taking appropriate, consistent action against those who commit fraud.

2.3 All the elements for achieving these objectives should be in place to achieve an integrated consistent approach to fraud risk management. This provides the best opportunity for the organisation to effectively:

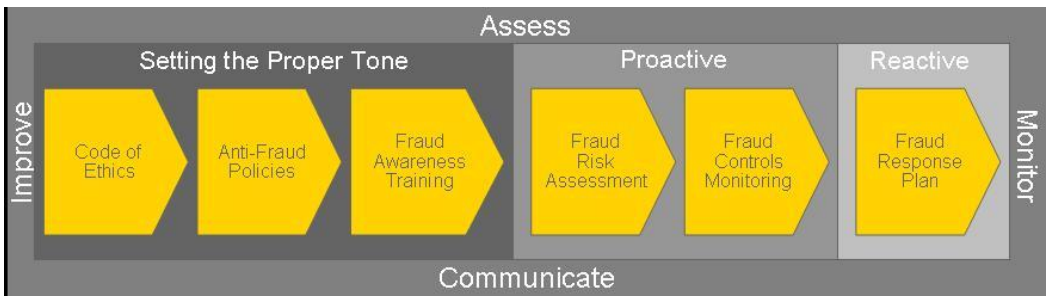
- Understand and mitigate current and emerging fraud threats faced by the organisation;
- Detect and investigate attempts to commit fraud against the organisation; and
- Respond to incidents or suspicions of fraud.

2.4 It should be noted that an anti-fraud governance framework will not provide absolute assurance against fraud but it can help to mitigate the effect of fraud.

Approach to review

2.5 We have performed a review of the anti-fraud governance framework which was in place in the States prior to May 2012, post August 2012 and after the assumed successful completion and embedding of the further planned actions detailed in the October 2012 States' Fraud Risk Management Improvement Plan.

2.6 Our approach to the review entailed each of the key anti-fraud governance framework elements, as depicted in the Ernst & Young anti-fraud governance framework model below:



2.7 The review used this model as a "starting point" against which the existing anti-fraud activities of the States were assessed, focusing on the three key areas of:

a) **Setting the proper tone** – including:

- ► the promotion of honest and ethical conduct through the use of a code of ethics;
- ► the establishment of anti-fraud policies that guide employees through complex issues; and
- ► fraud awareness training, educating employees on the organisation's code of conduct, understanding of the reporting process regarding suspicious activities, and communicating disciplinary actions that may be taken in the event of fraud.

b) **Proactive** – including:

- ► how the organisation currently identifies susceptibility to fraud; and
- ► the linkage of fraud risks to internal controls and assessing the effectiveness of controls to prevent and detect fraud.

c) **Reactive** – including:

- ► the investigation plan followed;
- ► the enforcement of uniform disciplinary procedures; and
- ► the existence of a fraud response plan.

2.8 We undertook a desktop review of anti-fraud documentation and interviewed key organisational stakeholders as directed by you or any of the interviewees.

2.9 By way of our desktop review and interviews, we have obtained an understanding of the anti-fraud governance framework, to identify strengths and weaknesses, and to allow the States to develop its approach in this area on an informed basis.

Review of documentation relating to anti-fraud

2.10 We reviewed documentation provided by the PAC, the States and interviewees. A list of documentation provided can be found at Appendix B.

2.11 In reviewing these documents, we have assessed their content (where relevant) against a baseline expectation for an organisation of similar size and complexity to the States. This baseline expectation is derived from our knowledge of working with a range of organisations in the area of anti-fraud, across a range of geographies and industries, in both private and public sector[4], and illustrates the key components of an effective anti-fraud governance framework for an organisation such as the States. We note that the States is currently seeking to move towards a more corporate approach to risk management.

2.12 We have not sought to independently validate or test the processes and controls detailed within the documents provided to us.

[4] See paragraph 5.4, we note that a counter-fraud maturity assessment was undertaken which suggested that the States were in the bottom 5-10% of public sector organisations across the UK.

Interviews

2.13 We conducted a series of structured interviews with key stakeholders across the organisation, as identified by the PAC or the interviewees themselves. A list of interviews conducted can be found at Appendix C.

2.14 We have not conducted detailed testing to independently verify the information provided during these interviews against documentary evidence.

2.15 Based on the output of the above, we have:

- Documented the States pre May 2012 anti-fraud governance framework;
- Documented the States post August 2012 anti-fraud governance framework;
- Documented the States future planned actions as part of the October 2012 States' Fraud Risk Management Improvement Plan;
- Undertaken a gap analysis between the anti-fraud governance framework after the future planned actions and our baseline expectation of an organisation of similar size and complexity; and
- Provided recommendations which will support and further enhance the States in determining the future direction and development of its priorities, including those recommendations and actions already identified as part of the October 2012 States' Fraud Risk Management Improvement Plan.

3. Ernst & Young anti-fraud maturity model

3.1 This section explains the Ernst & Young anti-fraud maturity model and details our summary assessment of the States' anti-fraud maturity within that model.

Ernst & Young anti-fraud maturity model

3.2 The Ernst & Young anti-fraud maturity model, developed through our work with clients in the anti-fraud area, comprises well defined states for assessing the capability of the States' anti-fraud activities. The model not only allows the States to assess its capability against organisations of similar size and complexity, but also to determine the improvements which can be made to:

- ► Bring this capability into line with organisations of equivalent size and complexity; or
- ► Achieve a desired state appropriate to the level of fraud risk faced by the States.

States' anti-fraud maturity model positioning

3.3 The maturity model illustrated on the next page is a graphic illustration of our summary assessment of the States' anti-fraud maturity within the Ernst & Young anti-fraud maturity model and represents our detailed findings set out in Appendix D (see Appendix E for further detail on the Ernst & Young anti-fraud maturity model).

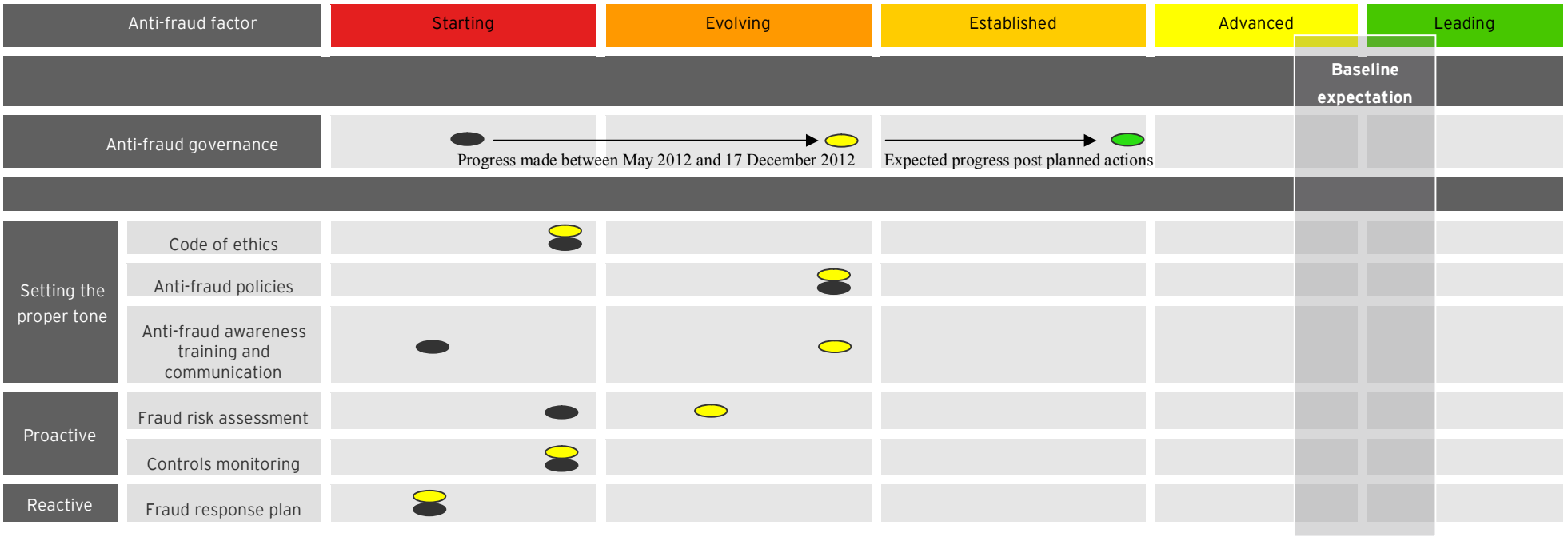
3.4 Broadly, our findings indicate that the States' anti-fraud framework position pre May 2012 was '**starting/ evolving**'.

3.5 The baseline expectation (reflecting organisations of equivalent size and complexity) is '**advanced/ leading**'.

3.6 Post August 2012, the state is '**evolving/ established**'.

3.7 Following the successful completion and embedding of the further planned actions detailed in the October 2012 States' Fraud Risk Management Improvement Plan, the States' would be expected to move further towards a position of '**established/ advanced**'.

Ernst & Young anti-fraud maturity model: Summary of the States' position for anti-fraud



Summary maturity model key

- The States' anti-fraud position pre May 2012
- The States' anti-fraud position post August 2012
- Anticipated anti-fraud governance "position" post successful completion and embedding of further planned actions detailed in the October 2012 States' Fraud Risk Management Improvement Plan

4. The appropriateness[5] of the States' anti-fraud governance framework pre May 2012

Introduction

4.1 This section considers the appropriateness of the States' anti-fraud governance framework pre May 2012 in comparison to an organisation of equivalent size and complexity.

Findings

Historic reports

4.2 An anti-fraud governance framework and risk management framework are interlinked; the former a subset, if not output, of the latter. A comprehensive risk management system requires the consideration of fraud and, for an anti-fraud governance framework to operate appropriately, it requires an organisation to have a fully embedded risk management system.

4.3 Over the last 12 years there have been a number of reports commissioned that have considered risk management at the States[6].

4.4 In 2006 the National Audit Office ("NAO") prepared a report on risk management and insurance in the States for the PAC ("the 2006 Report"). The report focussed on the effectiveness of the arrangements for risk management and assessed the progress made since the former States Audit Commission published a report in 2000 on risk management and insurance ("the 2000 Report").

4.5 The 2006 Report referred to a number of recommendations made in the 2000 Report, including that the States:

4.6 *"4.1.1 - Compile a comprehensive risk profile of the States, which identifies and prioritises key risks, assesses the adequacy of the present controls and highlights where insurance can be used effectively.*

4.7 *4.1.2 - Initiate a consistent and ongoing process for the identification and reporting of key risks by all States Committees."*[7]

4.8 The 2006 Report considered the 2000 Report recommendations and concluded that there had been *"a positive initial response to the Audit Commission's recommendations in 2000 and the States' approach to risk management has advanced over the last five years ... But there is scope for further progress. Risk management needs to be seen as part and parcel of everyday business, not as something different or separate or to be done as a special exercise. It is also important that risk management is regularly addressed at the highest levels within the States. Risk assessment must not be allowed to slip down the agenda or be left to be dealt with by junior staff within Departments."*[8]

[5] We note that the States does not have a defined risk management framework and communicated risk appetite. Therefore our approach to the review of the anti-fraud governance framework will be performed utilising our expectations of an organisation of equivalent size and complexity.

[6] See Appendix D, Ref 2 for further detail on structure and anti-fraud roles and responsibilities

[7] National Audit Office: "Risk Management and Insurance in the States of Guernsey" March 2006

[8] ibid

4.9 The NAO also noted that *"... without risks being regularly discussed at Board level, there is always a danger that key risks will be missed or will be tackled too late."*[9]

4.10 The NAO made a number of recommendations in relation to risk management at the States, including that:

4.11 *"g - A comprehensive risk profile of the States should be compiled, which identifies and prioritises the key risks ...*

4.12 *h – All Departments should review their methods of risk identification and prioritisation to ensure that they are in a position to deal with the threats that they may face."*[10]

4.13 We understand that initiatives were developed in response to this report, from 2006 onwards. In some Departments risk champions were designated, although with varying levels of success. We have been told that a risk manager was identified and began to undertake risk management work, but later left the role and momentum was lost. We understand that Departments did create corporate risk plans, but these were immature and inconsistent. They tended to focus on physical or operational risks (e.g. health and safety) rather than strategic, reputational or fraud risks.

4.14 Moreover, on 4 September 2009 the Welsh Audit Office published the Review of Good Governance, considering the governance arrangements at the States of Guernsey ("the WAO Report").The WAO Report included the following comments:

4.15 *"The lack of effective mechanism to implement policies and procedures across the States is a significant weakness in the current arrangements. It is critical that an effective separation of political and administrative accountability is realised. This would need a well-defined chain of command being put in place headed up by the Chief Executive who would need the authority to implement corporate initiatives and to hold civil servants accountable for their actions. It is difficult to envisage how this could be achieved without simultaneously addressing the issues of autonomy, authority and accountability within the existing political structures."*

4.16 *"Lack of clear leadership of and accountability within the Civil Service has a price. Inability to implement States-wide policies and procedures and ensure that there are consistent approaches to the way the States does business is exposing the States to financial and reputational risk."*[11]

4.17 We understand that a number of initiatives were developed subsequent to the WAO Report. In December 2010 the new Internal Audit Unit was created. In January 2011 the Chief Executive was given formal authority over Chief Officers, who became accountable to him but responsible to Ministers. From April 2011, more formal Chief Officer meetings were introduced, including quarterly reporting on risks, finance and departmental challenges.

4.18 However, in April 2012 a report, prepared by Deloitte LLP entitled "Review of Risk Management and Insurance", was published by the PAC ("the April 2012 Report"). The report followed up on the recommendations in the 2006 Report by the NAO and assessed the States current position with regards to risk management and insurance.

[9] ibid

[10] ibid

[11] Welsh Audit Office: Review of Good Governance – The States of Guernsey, dated 4 September 2009

4.19 It concluded that *"we found that the extent to which risk management had evolved within each of the Departments was largely dependent on the drivers within that Department (i.e. Clinical Governance or Health and Safety requirements) and the perceived value placed on the process by the relevant Chief Officer. We identified certain pockets of good practice around the capture and recording of risks but that from a corporate perspective, the initial focus and effort that existed following the NAO report in terms of identifying resource, training them in risk management and working to develop a States wide approach to risk had lost momentum and in some areas regressed to a pre 2006 position."*[12]

4.20 The April 2012 Report made a number of short, medium and long term recommendations. The short term recommendations were as follows:

"1 – Implement a simple, consistent Risk Management Framework across all departments and business areas which enable effective responses to risks and escalation where appropriate. Where possible this should build on the systems already in place in individual departments: As a minimum this should include:

a. The processes, methods and tools to be used for managing risk.

b. The way in which risk management performance will be measured and reported.

2 – Develop supporting policy and guidance applicable across all Departments to support managers throughout the States participate in Risk Management activities: As a minimum this should:

a. Consider the organisation's risk management objectives

b. Demonstrate a senior level commitment to risk management

c. Define accountabilities and responsibilities for managing risk

d. The periodic review and verification of the risk management policy and framework

3 – Develop a corporate risk management framework across the Executive Leadership Team and the Chief Officer Group which incorporates Department 'top risks' (where appropriate) and cross-cutting States wide strategic risks.

4 – Hold facilitated risk workshops at ELT[13] *and separately for each Department to develop a 'top down' view of the risks across each Department and establish a baseline for the risks faced by the Departments. In addition, the workshops could be used to 're-launch' risk management and provide business risk management training to staff and management across Departments.*

5 – Report on the outcomes and effectiveness of this process to the Policy Council on a regular basis."[14]

[12] Public Accounts Committee: "Review of Risk Management and Insurance" April 2012

[13] Executive Leadership Team

[14] Public Accounts Committee: "Review of Risk Management and Insurance" April 2012

4.21 Whilst the external reports described above did not specifically focus on anti-fraud or fraud risk, their findings and recommendations suggest that the States has repeatedly failed to implement and embed a consistent, formal, comprehensive approach to general risk management[15].

4.22 We understand that, whilst there were some pockets of good practice, generally risk management initiatives at the States have failed for a number of reasons. Financial and manpower restraints were highlighted to us, along with the States structure and a lack of consistency/ understanding of risk management and associated language amongst senior managers, which made it difficult to articulate and push through change.

4.23 We have also been told that, pre -2011, States Departments had greater autonomy, almost acting as a conglomerate of businesses, and that there was a cultural resistance to 'corporate centre' projects such as the drive to implement a risk management framework. We understand that this cultural resistance has diminished somewhat since 2011, and, indeed, some Chief Officers have expressed a desire for such a risk management framework.

4.24 Prior to the publication of the April 2012 report mentioned above, on 12 December 2011 the Internal Audit Unit ("IAU") Annual Report 2011 was published. It was circulated to the Chief Executive Officer, the Chief Officers, the Chief Accountant, the Head of Human Resources and Organisational Development, the PAC and the external auditors. We have been told that it was the first time a report of this nature was produced by the IAU[16].

4.25 The IAU Annual Report 2011 highlighted five common internal control concerns which had emerged during the internal audit activity in 2011. These concerns included the absence of a corporate risk management framework *"despite attempts to breathe life into this activity by the Policy Council"* [17], and also highlighted inconsistencies in dealing with common activities across the States, limited knowledge sharing and internal communications resulting in *"missed opportunities, unnecessary resistance and inefficiency"*[18] and that where corporate rules, directives and other initiatives have been established *"mechanisms and appetite for ensuring compliance by 'owners' does not always appear to be as robust as we would expect. Similarly, the legacy of decentralised management means that staff in departments do not always feel compelled to comply with activity and processes that were not created 'here'"*[19].

[15] We note that in October 2012 the States, acting through the Policy Council, commenced a procurement exercise for the provision of professional services to develop and implement a corporate approach to Risk Management across the States.

[16] We note that the new Internal Audit Unit was created in December 2010 and the practice of publishing annual reports was introduced in its first year of activity.

[17] Internal Audit Unit: "Annual Report 2011" December 2011

[18] ibid

[19] ibid

4.26 The fifth internal control concern highlighted was fraud risk:

4.27 *"Fraud risk – The primary responsibility for the prevention of fraud lies with management and those charged with governance of the organisation. It is important that management place a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals not to commit fraud because of the likelihood of detection and punishment. I believe that more needs to be done in both of these respects across the States."*[20]

4.28 We understand that this report was discussed with the Chief Executive and the Chief Accountant. The internal control concerns were recognised as long standing issues within the States and were considered reflective of the general "risk journey" the States was on at that time.

4.29 We note that the report did include the IAU Agreed Annual Plan for 2012, which incorporated a cross-cutting fraud risk review and a cross-cutting risk management review[21], amongst others. We have been told that this plan was developed by the Head of Internal Audit after consultation with management who acknowledged the deficiencies and the need for a plan to deal with them. We understand that it was hoped these reviews would provide a more detailed picture of the States' anti-fraud and risk management position at that time and would create a basis from which to move forward.

4.30 However, it is apparent from the above that, as at May 2012, the States was still lacking a consistent, formal, comprehensive and corporate approach to general risk management. This had clear implications for the management of risk generally and fraud risk specifically.

Appropriateness of anti-fraud governance framework pre May 2012

4.31 Appendix D includes a detailed analysis of the States' anti-fraud governance framework pre May 2012 and our detailed baseline expectation of an organisation of similar size and complexity for the purpose of comparison.

4.32 While there were elements of an anti-fraud governance framework, they were uncoordinated, inconsistent and not embedded culturally. In the context of the inconsistent approach to risk management across the States organisation it is perhaps unsurprising that we found the maturity of the pre May 2012 anti-fraud governance framework to be '**starting/ evolving**'[22].

4.33 The baseline expectation of an anti-fraud governance framework for an organisation of equivalent size and complexity is '**advanced/ leading**'[23].

4.34 Taking each of the three key areas of the Ernst & Young anti-fraud governance framework model in turn, our key findings are as follows:

[20] ibid

[21] We note that 'Risk Management' was on the IAU's initial 'key' reserve internal audit list. We understand that this was because the Head of Internal Audit wished to see the PAC 'Review of Risk Management and Insurance' and the action taken against that report before committing to a further review on the same subject.

[22] See Appendix E for further detail on the Ernst & Young anti-fraud maturity model

[23] ibid

Setting the proper tone

4.35 There was limited anti-fraud executive sponsorship or strategy.

4.36 There was no comprehensive, formal anti-fraud governance framework.

4.37 The existing anti-fraud policies were limited and, in places, contradictory. For example there was a lack of clarity over reporting lines for whistleblowers and in relation to responsibility for conducting investigations.

4.38 There was no single, central code of ethics applicable to every States employee.

4.39 There was a lack of fraud awareness training or communication of anti-fraud policies and whistleblowing procedures.

4.40 There was no requirement for States staff to sign an annual declaration of compliance with key policies, including the anti-fraud policy and code of ethics.

4.41 Third parties were not explicitly made aware of the States stance on fraud or how to raise concerns.

4.42 The culture was generally very trusting and naive with regard to fraud risk.

Proactive

4.43 A dedicated organisational fraud risk assessment had not been carried out.

4.44 The lack of a full fraud risk assessment resulted in fraud risks not being properly identified and hence fraud controls monitoring, beyond the developing work of the IAU, was ad-hoc in nature.

4.45 There was no process by which each Department or Committee had to complete a self-certification or provide evidence that it had identified and installed a system of internal controls (including with regard to anti-fraud) which was adequate for its own purposes, per the Statement of Internal Financial Controls in the States Accounts.

4.46 The use of data analytics had not been fully explored or aligned to fraud risks.

4.47 Detailed spend recovery audits, which are data analytics reviews of the accounts payable system to identify and recover fraudulent or erroneous historic supplier payments, were not conducted.

4.48 Anti-fraud management objectives were not explicitly included in the performance management process.

4.49 There was no collation, review or circulation of anti-fraud key performance indications, knowledge, management information or lessons learned from fraud experience.

4.50 Despite the lack of a risk management framework, guidance required Departments to make risk based decisions on the requirements for police checks on prospective recruits and for Procurement to make risk based decisions on due diligence on tendering companies.

Reactive

4.51 There was limited, high level fraud response guidance. No formal fraud response plan existed.

4.52 There was no corporate fraud investigation policy, procedures, standards, methodology or template documentation.

4.53 As fraud investigation and reporting was ad-hoc, it is not possible to tell if the enforcement of uniform disciplinary procedures occurred.

4.54 There was no central fraud investigation case management system.

Summary

4.55 We found that the States anti-fraud governance framework pre May 2012 was inappropriate compared to an organisation of similar size and complexity.

5. The reasonableness of the recommendations and actions set out in the internal audit reports issued in May 2012 and August 2012

Introduction

5.1 This section considers the reasonableness of the recommendations and actions set out in the internal audit reports issued in May 2012 and August 2012.

Findings

May 2012 Report

5.2 The IAU Annual Report 2011 highlighted five common internal control concerns, including fraud risk. In order to gain a better understanding of fraud risk within the States, the IAU Agreed Annual Plan for 2012 included a cross cutting review of fraud risk or 'Phase One' review.

5.3 The focus of the May 2012 report was anti-fraud governance mechanisms at a corporate/ strategic level and to assess how well anti-fraud activity was centrally managed and coordinated. This was a high level report, considering high level governance. It was anticipated that a number of Phase Two reports would follow. Phase Two would specifically focus on Departmental level assessments of fraud risk.

5.4 As part of the review a counter-fraud maturity assessment was undertaken. This suggested that the States were in the bottom 5-10% of public sector organisations across the UK. The report found that there were some anti-fraud resources and high levels controls, but little coordination or consistent oversight.

5.5 The four key areas of recommended improvement were:

- ► Develop the fraud rule, directive and guideline;
- ► Create a fraud risk register;
- ► Establish a corporate fraud lead; and
- ► Raise counter-fraud and ethics awareness.

5.6 The report assurance statement gave a "partial assurance"[24] rating in respect of corporate fraud risk management and governance. The definition of partial assurance was that there was a risk to the achievement of the objectives of the team, system, activity and/ or process and that some of the key controls are either missing or not operating effectively.

5.7 In October 2012, the recommendations detailed in the May 2012 report were developed into the States' Fraud Risk Management Improvement Plan by the Head of Internal Audit. The plan included 32 actions drawn from the original nine recommendations contained in the May 2012 Report. We have been told that the recommendations were accepted by the T&R Board. We note that, whilst progress has been made on a number of these recommendations and actions, some are

[24] We note that the levels of assurance that could be provided by the IAU were: Full, Moderate, Partial, No.

dependent on the appointment of a corporate fraud lead, which is still outstanding[25]. We believe this appointment should be made as a matter of priority.

5.8 We recommend that, given the historic low level of States anti-fraud maturity, the corporate fraud lead role should be a full time post. There is a risk that if the role is given to an individual with existing responsibilities, anti-fraud will not receive the time and focus required to ensure that the necessary improvements are made and that the anti-fraud culture is fully embedded.

August 2012 Report

5.9 We understand that the report was prepared by the Head of Internal Audit, in response to a request from the Chief Accountant, as an immediate reaction to the July 2012 alleged mandate fraud incident. We understand that this was a quick reaction review and was not exhaustive, although it resulted in a number of recommendations for improvement.

5.10 The objectives of the report were as follows:

- ► To assess the risks and the effectiveness of the risk mitigation associated with SAP payments and our current approach to authorisations;
- ► To identify opportunities to improve controls to ensure that all payments are correct and accurately reflected; and
- ► To reduce the potential exposure to the States through external fraud, departmental or T&R staff malpractice.

5.11 All recommendations were accepted by management and an action plan was created to ensure that the recommendations were implemented in a timely manner.

5.12 In response to the July 2012 alleged mandate fraud incident a series of improvements were made to the controls around the SAP payments system. These included the implementation of a number of immediate changes to controls which, we understand, were specifically designed to prevent a similar mandate fraud taking place again.

5.13 However, some of the actions identified in the August 2012 report were dependent on the Hub going live on 1 January 2013, resulting in a time delay before implementation. We have been told that, despite there being no States risk management framework in place, a risk based decision was made on each action that was delayed. We have been told that once the Hub is live, many processes that were formerly undertaken manually and across Departments will be automated and centralised.

Summary

May 2012 report

5.14 The recommendations and actions set out in the May 2012 report are not unreasonable.

5.15 However we believe some additional actions would be required to ensure that the States' anti-fraud governance framework would be appropriate for an organisation of similar size and complexity.

5.16 The additional actions identified form our recommendations in section 7.

[25] As at 17 December 2012, of the 32 action points listed, we have been told that 14 were 'complete' or 'largely complete', 12 were 'in progress' and 6 were dependant on the progress of other actions listed.

August 2012 report

5.17 The recommendations and actions set out in the August 2012 Report are not unreasonable.

6. The appropriateness[26] of the States' anti-fraud governance framework subsequent to these recommendations and actions

Introduction

6.1 This section considers the appropriateness of the States' anti-fraud governance framework subsequent to the successful completion and embedding of the further planned actions detailed in the October 2012 States' Fraud Risk Management Improvement Plan.

Findings

6.2 Appendix D provides a detailed analysis of the States' anti-fraud governance framework subsequent to the successful completion and embedding of the further planned actions detailed in the October 2012 States' Fraud Risk Management Improvement Plan.

6.3 Following the successful completion and embedding of the further planned actions detailed in the October 2012 States' Fraud Risk Management Improvement Plan, we anticipate that the States would move further towards a position of '**established**/ **advanced**'[27].

6.4 The baseline expectation of an anti-fraud governance framework for an organisation of equivalent size and complexity is '**advanced/ leading'**[28].

6.5 Taking each of the three key areas of the Ernst & Young anti-fraud governance framework model in turn, our key findings are as follows:

Setting the proper tone

6.6 The October 2012 States' Fraud Risk Management Improvement Plan includes many elements of an anti-fraud governance framework, however a number of these elements are still outstanding at this time. As at 17 December 2012, of the 32 action points listed, we have been told that 14 were 'complete' or 'largely complete', 12 were 'in progress' and 6 were dependant on the progress of other actions listed.[29]

6.7 There is evidence of anti-fraud executive sponsorship but this must be maintained in the face of competing priorities such as the Financial Transformation Programme. This sponsorship is vital in setting the proper tone at the top across the States and the corporate fraud lead must be visibly supported by the Chief Executive and the wider Executive Leadership Team on an ongoing basis. We recognise that it will be difficult for the corporate fraud lead, the Chief Executive and the Executive Leadership Team to drive change without clear and explicit political support and sponsorship.

[26] We note that the States does not have a defined risk management framework and communicated risk appetite. Therefore our approach to the review of the anti-fraud governance framework will be performed utilising our expectations of an organisation of equivalent size and complexity.

[27] See Appendix E for further detail on the Ernst & Young anti-fraud maturity model

[28] ibid

[29] In October 2012 the States, acting through the Policy Council, commenced a procurement exercise for the provision of professional services to develop and implement a corporate approach to Risk Management across the States.

6.8 We understand that a revised Corporate Fraud Rule and a revised Corporate Fraud Directive are being drafted. We have not seen these documents and refer to our recommendations in Appendix D with regard to their contents. The anti-fraud policies should be owned by the corporate fraud lead and aligned to existing policies.

6.9 There is no single, central code of ethics applicable to every States employee.

6.10 There is no requirement for States staff to sign an annual declaration of compliance with key policies, including the anti-fraud policy and code of ethics.

6.11 Anti-fraud awareness training has been developed and delivered to the SAP Support team and we understand that more than 50 staff of the Hub will receive classroom based support and training on 18 December 2012. A fraud awareness event is planned for early 2013. An ongoing anti-fraud awareness training and communication programme should be rolled out for all staff, beyond the fraud awareness event planned in early 2013. We understand that fraud awareness training and communication of anti-fraud policies or whistleblowing procedures does not form part of the induction process for all staff.

6.12 Specific anti-fraud training should be offered to staff in business areas that a full organisational fraud risk assessment deems are more susceptible to fraud and to those with defined anti-fraud roles.

6.13 Third parties are not explicitly made aware of the States stance on fraud or how to raise concerns.

6.14 We have been told that, historically, corporate initiatives have not always been fully embedded within Departments, limiting their value to the States as a whole. We believe consideration should be given to the establishment of a network of anti-fraud champions across Departments, to support the corporate fraud lead and mitigate the risk of Departmental resistance to anti-fraud initiatives.

6.15 There is greater anti-fraud awareness in the States. However, we understand that there is a limited culture of ownership of fraud awareness, detection and prevention across the organisation. Compliance with key policies and procedures is, at times, still considered optional.

Proactive

6.16 The IAU has undertaken, and is planning, a number of Departmental and process specific fraud risk reviews with a view to developing a self assessment process.

6.17 There is a lack of a dedicated organisational fraud risk assessment. The lack of a full fraud risk assessment means that organisational fraud risks are not being properly identified and this will negatively impact on the effectiveness of any fraud controls monitoring.

6.18 There is no process by which each Department or Committee has to complete a self-certification or provide evidence that it has identified and installed a system of internal controls (including with regard to anti-fraud) which is adequate for its own purposes, and which would support the Statement of Internal Financial Controls in the States Accounts.

6.19 This should form part of a self certification process supporting the statement of internal financial controls in the annual accounts.

6.20 The use of data analytics is still to be fully explored or aligned to fraud risks.

6.21 Standalone spend recovery audits, which are forensic data analytics reviews of the accounts payable system utilising historic fraud experience to identify and recover fraudulent or erroneous historic supplier payments, were not conducted[30].

6.22 Anti-fraud management objectives are not explicitly included in the performance management process.

6.23 There is limited collation, review or circulation of anti-fraud key performance indications, knowledge, management information or lessons learned from fraud experience. We understand that business intelligence and management information reports in relation to SAP are to be developed, in conjunction with users, by the SAP team.

6.24 Despite the continuing lack of a risk management framework, guidance requires Departments to make risk based decisions on the requirements for police checks on prospective recruits and for Procurement to make risk based decisions on due diligence on tendering companies.

Reactive

6.25 We understand that a formal fraud response plan is being drafted as part of the activity detailed in the October 2012 States' Fraud Risk Management Improvement Plan. We have not seen this document and refer to our recommendations in Appendix D with regard to its contents.

6.26 There is no specific central fraud investigation policy, procedure or standards. There is no defined standard investigation methodology or reporting template for corporate fraud investigations.

6.27 We understand that the formal fraud response plan which is currently being drafted will include consideration of the requirement for computer forensics.

6.28 There is no central fraud investigation case management system.

6.29 We understand that the corporate fraud lead will be expected to collate information on internal anti-fraud activity and share information on high profile fraud cases. However these plans do not explicitly include a process for the regular collation, review and circulation to specified personnel of knowledge, management information and anti-fraud key performance indicators. Establishing relationships with the fraud prevention community, both locally and in similar organisations, would support this process.

6.30 We understand that a "Raising Concerns at Work" policy is currently being developed. We have not seen this document and refer to our recommendations in Appendix D with regard to whistleblowing procedures.

6.31 Departments make risk based decisions on the requirements for police checks on prospective recruits or due diligence on tendering companies. Fraud risk due diligence on roles or procurement that is deemed high risk is not conducted by fraud investigation specialists.

[30] We have been told that the external auditors performed some data analytics as part of their audit work.

Summary

6.32 We found that subsequent to the successful completion and embedding of the further planned actions detailed in the October 2012 States' Fraud Risk Management Improvement Plan, the States' anti-fraud governance framework would be expected to move further towards a position of 'established/advanced'.

6.33 To meet our baseline expectation' as set out in the Ernst & Young anti-fraud maturity model, the States' anti-fraud governance framework would still require additional actions before being deemed appropriate compared to an organisation of similar size and complexity.

7. Recommended next steps

Introduction

7.1 This section of the report sets out our summary recommendations which will support the States in determining future anti-fraud direction and development priorities.

7.2 Our detailed recommendations can be found at Appendix D.

7.3 We note that the majority of our detailed recommendations are similar to, or an extension of, some of the high level recommendations and actions included in the October 2012 States' Fraud Risk Management Improvement Plan. However, in our view, the anticipated anti-fraud governance "position" post the successful completion and embedding of further planned actions detailed in the October 2012 States' Fraud Risk Management Improvement Plan, would still not meet our baseline expectation of an organisation of equivalent size and complexity. This is clear from the diagram in Section 3.

7.4 We understand that, as at the completion of our field work on 17 December 2012, of the 32 action points listed in the October 2012 States' Fraud Risk Management Improvement Plan, 14 were 'complete' or 'largely complete', 12 were 'in progress' and 6 were dependent on the progress of other actions listed. However we have not conducted detailed testing to confirm the completion of these actions. Appendix D provides a detailed overview of our understanding of the actions taken post August 2012, along with the further planned actions as at the date of the completion of our fieldwork and our additional recommendations.

Baseline

7.5 We note that the States does not have a defined risk management framework and communicated risk appetite. Therefore our review of the anti-fraud governance framework was performed utilising our expectations of an organisation of equivalent size and complexity as a baseline.

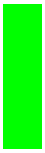
7.6 It is important to note that a leading practice anti-fraud governance framework is one which will develop and be enhanced over time. As the business and the environment within which it operates continues to change, and as the States' approach to anti-fraud matures and is fully embedded into the organisation, the anti-fraud framework will evolve, leading to an efficient, effective and consistent approach by the business in responding to fraud risk.

Recommendations

7.7 Our recommendations have, in discussion with you, been categorised as follows:

Priority recommendations for immediate to short term (starting within the next 6 months) implementation.

Recommended short to medium term implementation (starting within the next 12 months). These recommendations will often develop or follow on from the priority actions.



Desirable improvements to factor into longer term planning (starting within the next 18 months). These recommendations will support the continued enhancement of the States' anti-fraud governance framework.

Appendix D Reference	Baseline expectation	Summary Recommendation	Priority
1	Executive sponsorship and strategy	**A documented and approved anti-fraud governance framework ("AFGF") should be prioritised and embedded across the States.**	
1	Executive sponsorship and strategy	**The Executive Leadership Team must continue to actively push for the timely completion of the further planned actions.**	
1	Executive sponsorship and strategy	**The Executive Leadership Team must ensure that they continue to support this framework and strategy, and the work of the Corporate Fraud Lead once appointed, in an active and visible manner.**	
1	Executive sponsorship and strategy	**The Executive Leadership Team must ensure that those tasked with anti-fraud management have the necessary authority and ongoing support.**	
2	Structure	**Identify a corporate fraud lead.**	
2	Structure	**The revised structure should be incorporated into the revised Corporate Fraud Rule and revised Corporate Fraud Directive, clearly stating roles and responsibilities of identified individual(s).**	
3	Code of ethics	**Consideration should be given to the creation of a single code of ethics, based largely on the Civil Service Code that is applicable to all States Employees. It should include specific reference to fraud and the inclusion of defined sanctions for breaches.**	
4	Anti-fraud policy	**A single, clear anti-fraud policy should be implemented without delay.**	
5	Anti-fraud policy ownership	**The anti-fraud policy should be owned by the corporate fraud lead.**	

Appendix D Reference	Baseline expectation	Summary Recommendation	Priority
6	Policy framework	**The anti-fraud policy should be aligned with existing related policies.**	
11	Anti-fraud awareness & training - induction	**Anti-fraud policies and fraud awareness should be included in the States induction training for all staff.**	
12	Anti-fraud awareness & training – ongoing	**Develop and roll out formal anti-fraud awareness training and communication programme.**	
13	Anti-fraud training & awareness – enhanced training modules	**Specific anti-fraud training (for example Association of Certified Fraud Examiners) should be offered to staff in business areas that a full organisation fraud risk assessment deems are more susceptible to fraud or with defined anti-fraud roles.**	
15	Fraud risk assessment	**A full fraud risk assessment should be completed focussing on fraud schemes that are common to most organisations and those that are specific to the States and the business of each Department. The results should be incorporated into Departmental risk registers.**	
18	Data analytics	**A full spend recovery audit of the accounts payable system should be conducted to recover fraudulent or erroneous historic supplier payments.**	
20	Fraud response plan	**A formal fraud response plan should be implemented.**	
2	Structure	**Consideration should be given to the establishment of a network of anti-fraud champions across Departments, to support the corporate fraud lead.**	
7	Access to anti-fraud policies	**The anti-fraud policy and related policies should be made available to all States staff.**	

Appendix D Reference	Baseline expectation	Summary Recommendation	Priority
8	Policy communication	**The corporate fraud lead should be responsible for the ongoing communication of the anti-fraud policy and code of ethics to all staff on a regular basis.**	
9	Annual declarations	**An annual declaration of compliance with key policies, including the anti-fraud policy and code of ethics, should be implemented for all staff.**	
14	Anti-fraud training & awareness – third parties	**Ongoing management of key third party relationships to include a discussion of the States' expectations with regard to anti-fraud.**	
14	Anti-fraud training & awareness – third parties	**All framework agreements should include the States stance on fraud (i.e. zero tolerance) and details of how third parties can raise concerns (e.g. whistleblowing policy).**	
16	Fraud controls monitoring	**There should be ongoing assessment of the appropriateness of the design of controls identified as part of the full fraud risk assessment.**	
16	Fraud controls monitoring	**There should be ongoing assessment of the effectiveness of controls identified as part of the full fraud risk assessment.**	
17	Oversight and assurance	**Fraud risk should be specifically built into the self risk assessment process for each Department.**	
17	Oversight and assurance	**Fraud risk should form part of a self certification process with regard to the statement of internal financial controls in the annual accounts.**	

Appendix D Reference	Baseline expectation	Summary Recommendation	Priority
18	Data analytics	**Consideration should be given to opportunities available to introduce certain data analytics tests into the control environment, aligned to the key fraud risks identified.**	
19	Performance	**Objectives specific to anti-fraud management should be included in the performance management process of those States staff key to the implementation of the AFGF.**	
21	Fraud investigation	**Policy, procedures and standards to support the States in the completion of effective investigations should be produced.**	
23	Fraud investigation – computer forensics	**The corporate fraud lead, and any other individuals tasked with fraud investigation within the States, should complete first responder training.**	
26	Fraud response – lessons learned	**The fraud response plan should include a process to identify and disseminate lessons learned post investigation.**	
27	Whistleblowing procedures	**A clear whistleblowing policy should be established, including how to make reports and how the reports will be dealt with, and communicated to staff on an ongoing basis.**	
28	Management information	**The corporate fraud lead should centrally collate, review and circulate fraud related management information.**	
12	Anti-fraud awareness & training – ongoing	**Periodic surveys should be conducted to assess the level of fraud awareness across the States.**	

Appendix D Reference	Baseline expectation	Summary Recommendation	Priority
22	Adequately skilled resources	**The existing investigation skills and capability within the States should be evaluated, with a view to bringing that resource under the control of the corporate fraud lead.**	
24	Case management	**A basic case management system should be introduced.**	
25	Fraud intelligence	**The corporate fraud lead should review high profile fraud cases and communicate lessons learned which could be applied to the States.**	
25	Fraud intelligence	**The corporate fraud lead should establish relationships with the fraud prevention and investigation community, both locally and in similar organisations.**	
29	Key performance indicators	**Fraud related key performance indicators should be established and included as part of the management information.**	
30	Due diligence	**The corporate fraud lead should conduct fraud risk due diligence on any roles or procurement designated as high risk.**	
30	Due diligence	**Consideration should be given as to whether the States need to revisit the due diligence on existing relationships or employees.**	
31	Anti-fraud culture	**The Executive Leadership Team should closely monitor the anti-fraud culture across the States to ensure it is sufficiently robust and allows staff to raise relevant concerns, yet does not tie the States in cumbersome 'red tape'. This should be considered as part of the rollout of the corporate approach to general risk management.**	

Appendix A Scope of services

Extract from our engagement letter dated 30 October 2012:

In accordance with your instructions we will:

a) Through a review of previous reports, documentation and discussion with individuals as directed by you and as set out in Appendix B[31], or as supplied or directed by any of the individuals set out in Appendix B, and using the Ernst & Young anti-fraud maturity model, indicate the state of maturity of the States' anti-fraud governance framework pre-May 2012;

b) As set out in Appendix B, obtain previous reports or documentation on financial controls relating to fraud and risk management within the States of Guernsey, issued by internal audit, external audit, departments or officers of departments, other reviewers and the PAC, and, through discussion with individuals as directed by you or any of the individuals set out in Appendix B, understand the actions taken against the reports' findings and recommendations;

c) As deemed relevant by you, or any of the individuals set out in Appendix B, obtain copies of the Code of Conduct, Fraud Prevention Policies, Communication and Training, Fraud Risk Assessment, Controls Monitoring and Fraud Response Plan pertaining to the anti-fraud governance framework pre-May 2012;

d) Using our expectations of an organisation* of equivalent size and complexity, assess the appropriateness of the anti-fraud governance framework pre-May 2012;

e) Obtain the internal audit report issued in May 2012 and, through discussion with the Head of Internal Audit, the Ministers and staff from the Treasury & Resources Department and the Policy Council, as set out in Appendix B, understand the actions taken against its recommendations;

f) Obtain the internal audit report issued in August 2012 and, through discussion with the Head of Internal Audit, the Ministers and staff from the Treasury & Resources Department and the Policy Council, as set out in Appendix B, understand the actions taken against its recommendations:

g) Subsequent to the actions in (e) and (f) above, re-assess the appropriateness of the anti-fraud governance framework utilising our expectations of an organisation* of equivalent size and complexity;

h) Produce a findings and recommendations report on:

   I. The appropriateness* of the States' anti-fraud governance framework pre May 2012;

   II. The reasonableness of the recommendations and actions set out in the internal audit reports issued in May 2012 and August 2012;

   III. The appropriateness* of the States' anti-fraud governance framework subsequent to these recommendations and actions; and

   IV. Our recommended next steps, prioritised through discussion with you.

[31] The reference to Appendix B in the Scope of Services equates to Appendix C in this report.

* We note that the States does not have a defined Risk Management Framework and communicated risk appetite. Therefore our approach to the review of the anti-fraud governance framework will be performed utilising our expectations of an organisation of equivalent size and complexity.

We will conduct this work by way of a document review and interviews with individuals, as set out in Appendix B. For the avoidance of doubt, we will not conduct detailed testing to confirm either representations made or the embodiment and execution of the policies into procedures and processes at the departmental level.

If it is agreed that we should perform investigation work additional to that set out in this Statement of Work ("SOW"), we will agree with you in writing the scope of work and such subsequent agreement shall form part of a separate SOW.

Appendix B Documents provided to Ernst & Young

PAC defined "essential reports"

Internal Audit

Date	Body	Title
01.08.2012	Internal Audit Unit	Report
17.05.2012	Internal Audit Unit	Report
12.12.2011	Internal Audit Unit	IAU Annual Report 2011
2008	PriceWaterhouseCoopers	Internal Audit Findings Report
August 2007	Internal Audit	T&R: Treasury operations

Treasury & Resources Department

Date	Body	Title
July 2012	Chief Accountant, T&R	Report to Treasury & Resources Department

States of Guernsey

Date	Body	Title
13.09.2009	States of Guernsey	Rules for Financial and Resource Management v1.0 – Finance Rules: Fraud, p29
2008	States of Guernsey	The Civil Service Code

Public Accounts Committee

Date	Body	Title
May 2012	Deloitte LLP Report	Risk Management and Insurance in the States of Guernsey
January 2007	PAC - III 2007	Risk Management and Insurance in the States of Guernsey
March 2006	NAO Report	NAO Report on Risk Management and Insurance

External Auditors

Date	Body	Title
2012	Deloitte Report	Report on the PAC on the 2011 Audit - Final Report
111101	Deloitte Report	Report to the PAC on the 2011 Audit - Planning Report
110518	Deloitte Report	Report to the PAC on the 2010 Audit - Final Report
101103	Deloitte Report	Report to the PAC on the 2010 Audit - Planning Report
100609	Deloitte Report	Report to the PAC on the 2009 Audit - Final Report
091019	Deloitte Report	Report to the PAC on the 2009 Audit - Planning Report
090629	Deloitte Report	Report to the PAC on the 2008 Audit - Final Report
081016	Deloitte Report	Report to the PAC on the 2008 Audit - Planning Report
080630	Deloitte Report	Report to the PAC on the 2007 Audit - Final Report

PAC defined “possible useful reference reports”

Internal Audit

Date	Body	Title
2011	Internal Audit Unit	Formal Audit Charter
2011	Internal Audit Unit	States purchasing card governance
2009	PriceWaterhouseCoopers	States Internal Audit Plan
2009	Needham Partnership	Cross Departmental review of cash handling

Public Accounts Committee

Date	Body	Title
January 2012	Jim Brooks Consulting	Review of Financial Scrutiny in the States of Guernsey

Additional documents provided by the PAC, the States and interviewees and referred to in this report

Date	Body	Title
Various	T&R	Administrative and Accounting Guidelines
4 September 2009	Wales Audit Office	Review of Good Governance – The States of Guernsey
11 November 2011	States of Guernsey	Email from Director of Corporate Procurement to SAP Support team with link to BBC News article
August 2012	IAU	August 2012 Action Plan
29 August 2012	T&R	Email from the T&R Minister to Chief Officers with regard to Purchase Order compliance
September 2012	IAU	Internal Audit Update newsletter Issue 2
Undated (provided to E&Y on 12 November 2012)	IAU	May 2012 Action Plan
14 November 2012	States of Guernsey	Example letter sent to 7,000 States suppliers re Hub
19 November 2012	T&R	Email from States Treasurer sent to Chief Officers and Finance Directors, with regard to the October 2012 States' Fraud Risk Management Improvement Plan
Undated (provided to E&Y on 26 November 2012)	IAU	May 2012 Action Plan
17 December 2012	IAU	Proactive fraud management training slides
Undated (provided to E&Y on 17 December 2012)	IAU	May 2012 Action Plan
2012	IAU	Draft IAU Agreed Annual Plan

Appendix C Interviewees

Interviews conducted[32]

Treasury & Resources Department
Minister
Chief Accountant
Assistant Chief Accountant
Corporate Shared Service Director

Policy Council
Chief Minister
Chief Executive
Deputy Chief Executive
Head of HR & OD

Internal Audit
States Head of Assurance

External Audit
Lead Audit Partner
Audit Director

Other
Former Treasury & Resources Department Minister
Former States Treasurer

[32] Interviewees were identified by the PAC or by the interviewees themselves, in agreement with the PAC.

Appendix D Detailed findings and recommendations

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
1	Executive Sponsorship and Strategy Tone from the Top - A clear message from executive management on compliance with Anti-fraud Policy and related key policies and procedures (e.g. Fraud Response Plan, raising concerns). Executive management are able to demonstrate their involvement in anti-fraud management. Evidence of a comprehensive awareness campaign to communicate the anti-fraud message internally, driven by the executive management. Documented, approved and implemented Anti-fraud Governance Framework ("AFGF") addressing the management of fraud within the organisation. The anti-fraud strategy should be clearly linked to the overall strategic objectives of the organisation.	Prior to May 2012 there is limited evidence of a clear message from executive management in relation to anti-fraud management. There is limited evidence of a comprehensive, formal AFGF that had been documented, approved, implemented and embedded across the States. Where anti-fraud resources or high level controls were in place, there is little evidence that they were coordinated or that there was consistent executive management oversight. The IAU Annual Report 2011 highlighted five common internal control concerns, including fraud risk. In order to gain a better understanding of fraud risk within the States, the IAU Agreed	On 13 August 2012 at a Policy Council meeting, members agreed to establish an ad hoc Group consisting of Deputy St Pier, Deputy Luxon and Deputy Harwood to work with the Executive Leadership Team in reviewing corporate risk management across the States. We have been told that this Group will address fraud risk as part of wider corporate risk management. On 29 August the T&R Minister sent an email to Ministers and Chief Officers requesting that each Board formally endorse the adoption of the Purchase Order process at the next appropriate meeting,	As part of the October 2012 States' Fraud Risk Management Improvement Plan, an external consultant has been appointed to work with the States on implementation of the identified actions for improvement, , which includes many of the elements of an AFGF. We understand that a fraud awareness event is planned for early 2013 and executive management will be involved to demonstrate tone from the top.	**A documented and approved AFGF should be prioritised and embedded across the States.** **The Executive Leadership Team must continue to actively push for the timely completion of the further planed actions.** **The Executive Leadership Team must ensure that they continue to support this framework and strategy, and the work of the Corporate Fraud Lead once appointed, in an active and visible manner.** **The Executive Leadership Team must ensure that those tasked with anti-fraud management have the necessary authority and**

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		Annual Plan for 2012 included a cross cutting review of fraud risk or 'Phase One' review. This resulted in a report, published in May 2012, which focussed on anti-fraud governance mechanisms at a corporate/ strategic level and assessed how well counter-fraud activity is centrally managed and coordinated. It identified four key areas of recommended improvement: ► Develop the fraud rule, directive and guideline; ► Create a fraud risk register; ► Establish a corporate fraud lead; and ► Raise counter-fraud and ethics awareness.	with a view to increase the usage of Purchase Orders by Departments from a rate of around 40% to over 90% or over. This demonstrated tone at the top with regard to Purchase Order compliance. The recommendations detailed in the May 2012 report developed into the October 2012 States' Fraud Risk Management Improvement Plan. While progress has again been made on a number of the actions, some are dependent on the appointment of a corporate fraud lead, which is still outstanding. The States Treasurer sent a communication on 19 November 2012 to a number of Chief Officers and their Financial Directors. The communication		**ongoing support.**

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
			explained the status of the October 2012 States' Fraud Risk Management Improvement Plan, emphasising the importance of the work and demonstrating tone from the top.		
2	Structure Anti-fraud roles and responsibilities are clearly defined in terms of strategy, intelligence, analytics, prevention, detection, reporting and investigation. Overall responsibility for the coordination of the anti-fraud strategy is delegated by the Chief Executive to an appropriate individual within the organisation, providing an internal focal point to the organisations anti-fraud programme.	Prior to 2011 there had been a lack of clarity over roles and responsibilities and interviewees noted that it had long been recognised that the structure of the States of Guernsey needed to be reviewed. Each Department had a finance team which reported to the Chief Officer of that Department and not to the Chief Accountant. As a result, we understand that the Chief Accountant did not have the ability to exercise control over the financial functioning of each Department.	On 22 September 2012 it was announced that certain senior civil service responsibilities were to be restructured. The Head of Human Resources and Organisational Development, was appointed to a new and broader role of States Chief Corporate Resources Officer. This new role extends the existing remit to include responsibility for all non-financial resources, including property, IT and the	Options for the role of a corporate fraud lead, along with terms of reference and potential job description are being prepared as part of the fraud improvement work package. A corporate fraud lead is yet to be identified.	**Identifying a corporate fraud lead should be an absolute priority.** Other actions are dependent on the appointment of this role and should not be delayed. The corporate fraud lead should: ► Bring focus, energy and commitment to anti-fraud management in the States; ► Champion the benefits of anti-fraud management; ► Be a central reporting

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		In addition, T&R had both a Chief Accountant and a Chief Officer, further complicating lines of reporting and responsibility. In February 2011 the contracts of Chief Officers were amended to create a direct reporting line to the Chief Executive. The States of Guernsey Rules for Financial and Resource Management states that: "States members sitting as the States of Deliberation are responsible for approving ... the framework of the Rules for Financial and Resource Management [and] the Finance, Property, Procurement, ICT and Cross-cutting Rules."[33] "The Treasury and Resources Department has responsibility for	new shared transactional services centre known as "the Hub". The role of States Treasurer has been reintroduced. The remit of this role now extends to cover responsibility for all financial matters, including responsibility for corporate procurement and the Income Tax Office. The States Chief Corporate Resources Officer and States Treasurer provide advice to the Policy Council as well as the Treasury & Resources Department, and work across the States. They report directly to the Chief Executive. The Head of Internal Audit took on additional		point for suspected fraud or unethical behaviour; ► Lead and manage the States response to allegations of fraud or unethical conduct in accordance with fraud response plan; ► Identify, review and circulate fraud intelligence; ► Assist Departments to create and maintain an anti-fraud culture; ► Ensure employees, contractors, partners and suppliers are engaged in combating fraud and unethical behaviour; ► Measure and report on fraud experience; ► Support fraud risk assessments at a Departmental level; ► Conduct overall

[33] States of Guernsey Rules for Financial and Resource Management Finance Rules: Roles and Responsibilities

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		...reviewing the Rules on a cyclical basis (at least every three years and approving changes or recommending new Rules to the States as appropriate ... reviewing the framework of the States Rules for Financial and Resource Management and recommend changes to the States as appropriate ... reviewing and approving Directives prepared by Heads of Profession following a consultation process."[34] It also states that the T&R Department mandate includes "risk management."[35] Departments' responsibilities include "to identify and install internal control systems, including financial control systems,	responsibility for corporate assurance activities and the risk champion role, in an extended role as States Head of Assurance. This role also now reports directly to the Chief Executive. While the restructuring is not specifically designed to reduce fraud risk, it is intended to ensure standards and policies are applied consistently and that there is accountability. Existing anti-fraud roles and responsibilities have been examined and considered as an initial step in considering the corporate fraud lead		organisational fraud risk assessment; and ► Share good anti-fraud practice. Given that the historic low level of States anti-fraud maturity we believe the corporate fraud lead role should be a full time post. There is a risk that if the role is given to an individual with existing responsibilities, anti-fraud will not receive the time and focus required to ensure that the necessary improvements are made and that the anti-fraud culture is fully embedded. **Consideration should be given to the establishment of a network of anti-fraud champions across**

[34] ibid

[35] ibid

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		to safeguard public funds and resources."[36] Chief Officers are responsible for "ensuring there are robust internal controls (procedures, performance management and monitoring systems) in place to enable compliance with the Rules and Directives."[37] The States of Guernsey Rules for Financial and Resource Management - Finance Rules: Fraud state that "Senior Finance Officers must ensure that their Departments operate robust internal controls which prevent fraud and minimise the potential for fraud or other irregularity to remain undetected. All States employees are expected to be aware of and vigilant for suspicious or improper activities." [38]	role.		**Departments, to support the corporate fraud lead.** Anti-fraud champions would provide insight at a Departmental level and tackle any resistance at Departmental level to corporate initiatives. They would help the corporate fraud lead ensure consistency across Departments and prevent a silo approach to anti-fraud management. The anti-fraud champion role would involve minimal time commitment. **The revised structure should be incorporated into the revised Corporate Fraud Rule and revised Corporate Fraud Directive, clearly stating roles and responsibilities of**

[36] ibid

[37] ibid

[38] States of Guernsey Rules for Financial and Resource Management - Finance Rules: Fraud

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		However there are some contradictions with regard to certain anti-fraud roles and responsibilities. See point 4 below entitled anti-fraud policy for further detail on contradictory reporting lines.			**identified individual(s).**
3	Code of ethics A code of ethics should promote honest and ethical conduct. It should address issues such as compliance with applicable laws, rules and regulations and the prompt internal reporting of any breaches of the code. To ensure all employees are aware of the code, it should be highlighted on induction and at least once annually, for example by way of an annual declaration of compliance to the code signed by each employee. It should be made clear that all employees are held accountable for adherence to the code and the defined sanctions imposed in cases of non-compliance explicitly stated.	We were told by the majority of interviewees that the Civil Service Code was equivalent to a code of ethics. It details four core values for the Civil Service: integrity, honesty, objectivity and impartiality. It notes that civil servants should comply with the law. However it makes no specific reference to fraud. In addition the Civil Service Code does not detail the sanctions that may be imposed if it is not followed (i.e. whether it is treated as a significant breach/gross misconduct and subject to disciplinary	No changes have been made to the Civil Service Code.	We are not aware of any further planned actions.	The lack of a single central code of ethics that is applicable to every States employee, regardless of role, could lead to confusion and inconsistency. An organisation is only as strong as its weakest link. Every States employee should be expected to act in an ethical manner. While we recognise that there are certain aspects of the Civil Service Code that may not be relevant to other States employees, **we would recommend that consideration is given to**

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		action). We note that the May 2012 report included a staff perception survey on the subject of fraud and malpractice. The survey found that, while 69% of respondents said they were aware of a professional code of ethics, "only 18% named the Civil Service Code as fulfilling this function." [39] Three of our interviewees were unable to name a States equivalent to a code of ethics. As the title of the document implies, the Civil Service Code details core values for civil servants. It also notes that "individual Departments and Committees may also have their own separate mission and values			**the creation of a single code of ethics, based largely on the Civil Service Code that is applicable to all States employees.** The new code of ethics should include specific reference to fraud and the inclusion of defined sanctions for breaches. This code should be rolled out as part of the launch of the new AFGF. The code should be provided to all existing States staff and should be covered in all induction training.

[39] May 2012 report, page 17, paragraph 99

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		statements based on the core values."[40]			
4	Anti-fraud policy Anti-fraud policy has been established and approved by executive management. The policy is specific to the organisation, and includes: ► Guidance for employees through complex issues and procedures that govern the escalation of fraud allegations; ► Support/protection provided by the organisation for whistleblowers; and ► Confidentiality observed during investigation. The policy contains relevant definitions and shows the relationship between other relevant policies i.e. code of ethics. The policy is structured in a clear and concise manner, stating to whom it applies. Mandatory elements of the policy are clearly separated from guidance. Consequences of non-	There were two documents that addressed elements of an anti-fraud policy. The first was the States of Guernsey Rules for Financial and Resource Management Finance Rules: Fraud ('the Fraud Rule'). The Fraud Rule we were provided was last updated on 13 October 2009. It is a single page, setting out the responsibility for preventing, reporting and investigating fraud along with the consequences of committing fraud. The Fraud Rule is marked mandatory. The second document is the Administrative and Accounting Guideline: Fraud and Other Irregularities ('the Fraud	We understand that no changes have been made to the Fraud Rule or Fraud Guideline.	We understand that a revised Corporate Fraud Directive and Corporate Fraud Rule are currently being drafted as part of the fraud improvement work package and will be launched as part of the fraud awareness event in early 2013.	**A single, clear anti-fraud policy should be implemented without delay.** This policy should include: ► A statement outlining the purpose of the policy; ► A clear definition of what is meant by fraud, with relevant examples. For example, the States may define fraud as 'an intentional act, of deceit, to obtain unjust/illegal advantage'. A relevant example of what is meant by fraud may include; 'the deliberate submission of non-business

[40] Civil Service Code, paragraph 3

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
	compliance are set out. Requirements and terminology within the anti-fraud policy are consistent with other policies.	Guideline'). We have been told that, historically, the Administrative and Accounting Guidelines were not mandatory. However we have been told that on adoption of the Rules for Financial and Resource Management (including the Fraud Rule) after approval by the States of Deliberation in November 2009, the Administrative and Accounting Guidelines became mandatory, until such time as they were replaced by Directives, which would also be mandatory. We note that the Fraud Guideline we were provided is dated 'Jun 95', that it does not refer to being mandatory in nature and that it still includes the text "this guideline is intended to provide guidance to all States			related, exaggerated or fictitious expenses with the intention of obtaining reimbursement for those expenses from the States'; ► An articulation of the States' position on fraud and unethical behaviour e.g. no tolerance, and that all potential incidents of fraud (i.e. where intent has been established) are to be reported immediately to the corporate fraud lead; ► A clear scope of the policy and to whom it applies e.g. staff, contractors, suppliers; ► An explanation of how the States will respond to fraud, including escalation of incidents reported (this should be consistent with the States' Fraud

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		employees."[41] We understand that a draft Fraud Directive existed prior to May 2012, but had yet to be implemented. We were told that Directives are introduced after a period of consultation with all Departments. We understand that this consensus approach can result in delays and that Directives are therefore grouped in batches for the sake of efficiency. The Fraud Rule advises that an employee who suspects fraud is occurring, or that there may exist a high potential risk of fraud, should report their concerns immediately to the Chief Accountant and the Head of Internal Audit. The Fraud Guideline advises			Response Plan) ► A statement regarding confidentiality , both during investigations and during subsequent reporting; ► A statement on the publication policy of any sanctions applied; ► Details of the channels through which staff, contractors and suppliers can raise concerns; ► An explanation of how whistleblowers will be protected including information on how staff can raise concerns, and addressing issues such as 'what happens if I report a genuine concern which is subsequently

[41] Administrative and Accounting Guideline: Fraud and Other Irregularities

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		that an employee should bring their concerns to the attention of their immediate line manager, if their line manager is implicated, to the Chief Officer or the most senior officer available. If the Chief Officer is implicated, the Fraud Guideline notes that the employee should report their concerns to the Chief Internal Auditor or the States Treasurer. The Fraud Rule notes that Internal Audit is responsible for the investigation of fraud. The Fraud Guideline does not make specific reference to responsibility for investigation but notes that the Chief Officer, the Chief Internal Auditor and a representative of the Guernsey Police should meet to discuss the most appropriate action, but that the responsibility for the course of action to be taken will at all times rest with the employing			found not to be an issue?; ► Consequences of non-compliance with the policy; and ► Identification of related policies applicable to all staff e.g. code of ethics, expenses policy, and information security policy. The anti-fraud policy should be communicated at induction and on an ongoing basis, for example by way of an annual compliance declaration. It should be easily available to all States staff. It should be clearly and concisely drafted, without ambiguity.

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		Committee.			
5	Anti-fraud policy ownership Ownership of policies is clearly identified. The impact on the anti-fraud policy of changes to other policies should be considered and, if appropriate, changes should be made. Anti-fraud policy changes should consider practical business requirements but should also be timely in their implementation.	The framework for the States Rules for Financial and Resource Management are as follows: ► The Rules are prepared by T&R Department and agreed by the States of Deliberation. They are mandatory. ► The Directives are prepared in consultation with Departments, issued by the Heads of Profession and approved by T&R Department. They are mandatory. ► Guidance on specific areas is written in consultation with Departments and issued by the Heads of Profession. Guidance is not	No changes have been made to the ownership of policies.	We are not aware of any further planned actions.	**The anti-fraud policy should be owned by the corporate fraud lead.** Where gaps or inconsistencies are identified, the anti-fraud policy should be updated as soon as practicable. It should be reviewed on an annual basis to ensure there is no requirement for revision.

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		obligatory. ► Procedures are formulated by each Department and must comply with the Rules and Directives. ► The States Treasurer owns the Rule and the Directive.			
6	Policy framework The anti-fraud policy should sit within a suite of policies which support the AFGF. Relevant policies may include: ► Expenses; ► Code of Ethics; ► Grievance and disciplinary; ► IT Security; ► Data privacy; and ► Fraud Response. Policies are clear and concise and the specific requirements are consistent with the approach	There was a lack of overall coordination of the wider policy framework from an AFGF perspective. The Code of Ethics is addressed separately at point 3 above. The Fraud Response Plan is addressed separately at point 20 below.	We understand that a review of Human Resources Policies is being carried out but that no changes have been made to the wider policy framework in support of AFGF.	We understand that consideration will be given to the integration of the revised Corporate Fraud Rule and revised Corporate Fraud Directive with other relevant policies as part of the fraud improvement work package.	**The anti-fraud policy should be aligned with existing related policies.** Amendments to existing policies may be required when the revised Corporate Fraud Directive and Corporate Fraud Rule are introduced. It should be ensured that the Corporate Fraud Directive and Corporate Fraud Rule reference relevant related policies. They should be consistent with the requirements stipulated in other relevant

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
	outlined in the anti-fraud policy.				policy documentation.
7	Access to the anti-fraud policy Anti-fraud policies are accessible to all staff	There was no single, clear, comprehensive anti-fraud policy. We understand that the Fraud Rule and the Fraud Guideline were accessible on the Intranet. We note that the Intranet was not accessible to all States staff.	We understand no change has been made to the availability of the Fraud Rule and Fraud Guideline.	We are not aware of any further planned actions.	**The anti-fraud policy and related policies should be made available to all States staff.** Storing, accessing and updating policy documentation electronically is preferable to retention of hard copies. Where all staff do not have access to online documentation, measures should be taken to ensure all are aware of mandatory anti-fraud requirements, the consequences of failing to comply and where they can access further information.

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
					Use of existing communication channels within the States should be considered.
8	Policy communication The anti-fraud policy and code of ethics are communicated to all staff on a regular basis including at induction, annually thereafter and following any significant change, amendment or addition to the policies.	We understand that there were limited communication channels for the dissemination of anti-fraud information. The Civil Service Code was highlighted at induction training but the induction training did not specifically cover anti-fraud policies or fraud awareness.	We understand no change has been made to the communication of the Fraud Rule, Fraud Guideline or the Civil Service Code.	The fraud awareness event in early 2013 will communicate the revised Corporate Fraud Rule and revised Corporate Fraud Directive. A presentation and communications plan is part of the fraud improvement work package.	**The corporate fraud lead should be responsible for the ongoing communication of the anti-fraud policy and code of ethics to all staff on a regular basis.** Consideration should be given to the use of multiple communication channels on an ongoing basis. Effective combinations of communications channels can include intranet, electronic circulation of policy documentation (often accompanied by annual declarations of compliance) reference to policies as part of other States training programmes (e.g. induction, new manager training, anti-fraud training) and discussion or

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
					reference to anti-fraud policies by management in team meetings or staff forums.
9	Annual declarations All staff required to sign an annual declaration of compliance with key policies, such as anti-fraud, code of ethics and IT security.	We have been told that the States did not require staff to sign an annual declaration of compliance with key policies.	We understand no change has been made since the August 2012.	We are not aware of any further planned actions.	**An annual declaration of compliance with key policies, including the anti-fraud policy and code of ethics, should be implemented for all staff.** This process will help maintain awareness of the existence of key policies and the requirements within those policies which must be adhered to by all staff. Completion of the annual declaration process should be monitored and non-compliance with the declaration process followed up. The process could be completed manually or electronically, and should be tailored to those

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
					working outside of an office environment. Where possible the method of communication should leverage existing communication channels, such as team meetings, mandatory annual training refreshers, visits to the office, all staff briefings etc.
10	Terms of employment and disciplinary process Gross misconduct, as defined by the grievance and disciplinary policy, clearly identifies the act of fraud as a behaviour which constitutes gross misconduct. This is consistent with staff contracts of employment. The standard contract of employment states that computer systems, equipment and associated electronically stored data, including emails, remains at all times the property of the organisation unless explicitly stated otherwise.	We understand that the grievance and disciplinary policy identified the act of fraud as behaviour which constitutes gross misconduct. We understand that, while there is no single standard contract of employment, the Rules and Directives are contractual across the States. The IT Directives state that all electronic data remains at all times the property of the States.	We understand no change has been made since the August 2012.	We are not aware of any further planned actions.	We have no further recommendations on this point.
11	Anti-fraud awareness training and	We understand that	We understand that	We are not aware of	**Anti-fraud policies and**

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
	communication – induction New staff induction module covering anti-fraud policies and fraud awareness.	induction training and communication did not cover anti-fraud policies or fraud awareness. We note that induction training for Civil Servants did highlight the Civil Service Code.	anti-fraud policies and fraud awareness have been added to the induction training for new members of the Hub. However anti-fraud policies and fraud awareness is not currently part of the induction training for States staff outside this team. It should be noted that a large number of payments are still made by States Departments outside of the SAP team.	any further planned actions.	**fraud awareness should be included in the States induction training for all staff.**
12	Anti-fraud awareness training and communication – ongoing Coordinated anti-fraud awareness campaign developed and implemented across the organisation. Awareness programme kept relevant and up to date over time. Awareness programme utilises various existing communication channels within the	We have been told that there was limited ongoing anti-fraud awareness training and communication in the States.	We note that the September 2012 Internal Audit Update newsletter highlighted fraud risk, alongside other risks, and the work the IAU was doing in this area. It invites those with any concerns about fraud	A fraud awareness event is planned for early 2013. Anti-fraud awareness and related resources intranet area is currently under development	**Develop and roll out formal anti-fraud awareness training and communication programme.** All States staff are expected to be aware of and vigilant for fraud. However they need to be

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
	organisation. Communications and alerts regularly distributed highlighting relevant issues and potential indicators of fraud are shared. Regular anti-fraud training provided across the organisation. Training programme attendance is monitored. Training programme is kept relevant and up to date and tailored, as appropriate, for employees within different Departments.		risk in their business area to contact the Head of Internal Audit. Operational fraud awareness training material has been developed. Fraud awareness training has been delivered to existing members of the SAP support team. Fraud awareness presentation materials have been provided to the SAP training team for inclusion in sessions for relevant staff. It should be noted that a large number of payments are still made by States Departments outside of the SAP team.	by the IAU. Fraud awareness training will be delivered to more than 50 members of the Hub on 18 December 2012. Additional fraud awareness sessions are being discussed with a number of Departments. The IT Security Officer has submitted a bid for a software package to deliver computer based training that could have use and value in communicating anti-fraud awareness to staff.	properly equipped to recognise indicators of fraud and how to raise concerns. All civil servants should receive training in anti-fraud policies and fraud awareness. Other States staff should receive training based in line with a fraud risk assessment of their Department. An organisation is only as strong as its weakest link. Every States employee has a role to play in the prevention of fraud. Failure to provide training for staff can result in weak points in the States anti-fraud defences. The outcomes of investigations and disciplinary actions in relation to fraud should, where appropriate, be shared. This would demonstrate action taken, boost staff

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
					confidence in reporting concerns and act as a deterrent to potential fraudsters. It would reduce any perception that fraud would not be detected or prosecuted. **Periodic surveys should be conducted to assess the level of fraud awareness across the States.** The results of these surveys can be used to direct enhanced training and awareness efforts, as required.
13	Anti-fraud awareness training and communication – enhanced training Specific anti-fraud training is offered to staff in business areas which are more susceptible to fraud or with defined anti-fraud roles.	We understand that enhanced anti-fraud training was ad-hoc.	The Head of Internal Audit has raised fraud risk awareness within the IAU team to ensure that they remain alert to the risk of fraud in each internal audit engagement that they undertake.	The Head of Assurance will seek to obtain a formal, counter-fraud qualification in 2013. Consideration will be given to the design and delivery of additional anti-fraud training to Chief Officers and Senior	**Specific anti-fraud training (for example Association of Certified Fraud Examiners) should be offered to staff in business areas that a full organisation fraud risk assessment deems are more susceptible to fraud or with defined anti-fraud**

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
				Finance staff. Consideration will be given to additional fraud risk training requirements across the States.	**roles.**
14	Anti-fraud awareness training and communication – third parties The anti-fraud stance of the organisation is communicated to key third parties as part of the ongoing relationship with those parties. Third parties are made aware of any contractual obligations requiring reporting of potential fraud incidents, and the lines through which these issues should be reported. The organisation explicitly discusses expectations related to fraud and unacceptable behaviour, as well as encourages reporting of unusual or fraudulent activities with key third parties.	We have not seen any evidence that the States anti-fraud stance was communicated to key third parties as part of the ongoing relationship with those parties.	A letter was sent to all States suppliers' to inform them of the implementation of the Hub and the requirements for Purchase Order references on all invoices.	We are not aware of any further planned actions.	**Ongoing management of key third party relationships to include a discussion of the States' expectations with regard to anti-fraud.** **All framework agreements should include the States stance on fraud (i.e. zero tolerance) and details of how third parties can raise concerns (e.g. whistleblowing policy).** This will help ensure that the States only do business with those third parties who share the same ethical standards.

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
15	Fraud risk assessment A dedicated fraud risk assessment is performed, focussing on fraud schemes that are: ► Common to most organisations; and ► Specific to this organisation and the business of each Department, as relevant. The assessment identifies key fraud risks potentially facing the organisation, mitigating controls and likely impact for each area of the business. The results are communicated to executive management. Review of fraud risks and related controls includes consideration of fraud risks associated with key third party relationships.	A dedicated organisational fraud risk assessment had not been carried out. General risk assessments have been conducted in a number of Departments but have been inconsistent in approach. While there were some pockets of good practice, the risk assessments tended to focus on physical risks and health and safety rather than fraud risk. Fraud risk has been considered in previous internal audit reviews.	Fraud has been included in the T&R risk register as a potential risk. The IAU is carrying out 'Phase 2' reviews which include a thematic fraud risk assessment of Procurement. A tendering process is currently being undertaken for a consultant to support a corporate approach to general risk management.	We understand further IAU Phase 2 reviews are planned for 2013. It is intended that these reviews will contribute to the creation of a self assessment fraud risk pack that will allow Departments to conduct their own fraud risk reviews going forward. Fraud risk will also feature as an element of the scope of the majority of internal audits planned in 2013.	**A full fraud risk assessment should be completed focussing on fraud schemes that are common to most organisations and those that are specific to the States and the business of each Department.** **The results should be incorporated into Departmental risk registers.**
16	Fraud controls monitoring Internal controls are linked to fraud risks identified during the fraud risk assessment	A lack of full fraud risk assessment means that fraud risks have not been properly identified and hence any fraud controls monitoring was ad-hoc in nature. The IAU considered fraud risk as part of their audit	We understand no change has been made since August 2012.	We are not aware of any further planned actions.	**There should be ongoing assessment of the appropriateness of the design of controls identified as part of the full fraud risk assessment (see point 15 above).** **There should be**

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		planning.			**ongoing assessment of the effectiveness of controls identified as part of the full fraud risk assessment (see point 15 above).**
17	Oversight and assurance Formal process of monitoring compliance with fraud controls as part of general monitoring of framework e.g. internal audit reviews or self risk assessment process	The IAU recognised fraud risk in the 2011 IAU Annual Report and scoped it into the internal audit plan for 2012. In May 2012 the IAU published a report highlighting concerns about fraud risk management and anti-fraud maturity at the States. There was limited evidence of fraud risk self assessments across Departments. We note that the States Accounts 2011 include a Statement of Internal Financial Controls. This notes that "it is the responsibility of each	Per point 15 above, the IAU is carrying out a number of 'Phase 2' reviews which include a thematic fraud risk assessment.	In addition to specific fraud risk reviews, fraud risk will also feature as an element of the scope of the majority of internal audits planned by the IAU in 2013 (see point 15 above).	**Fraud risk should be specifically built into the self risk assessment process for each Department.** **Fraud risk should form part of a self certification process with regard to the statement of internal financial controls in the annual accounts.**

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		States Department and Committee to identify and install a system of internal controls, including financial control, which is adequate for its own purposes."[42] However we understand that there is no process by which each Department or Committee has to complete a self-certification or provide evidence to confirm this statement.			
18	Data analytics Use of data analytics to identify 'red flags' in the organisations transactions that may indicate fraudulent activity. Spend recovery audits conducted on accounts payable systems.	The external auditors performed some data analytics as part of their audit work, e.g. journal entry testing. We have been told that this work included consideration of duplicate payments, possible fraudulent payments and ghost employees.	We understand no change has been made since August 2012.	Discussions are planned between the SAP Business Intelligence Manager and the Head of Internal Audit to develop SAP queries related to fraud risk.	**Upon completion of the fraud risk assessment (point 15 above), consideration should be given to opportunities available to introduce certain data analytics tests into the control environment, aligned to the key fraud risks identified.** **A full spend recovery audit of the accounts**

[42] States of Guernsey Accounts 2011

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
					payable system should be conducted to recover fraudulent or erroneous historic supplier payments. This exercise should be forensic and fraud risk focussed. It should be undertaken outside of the traditional external audit process. Data analytics should also include consideration of fraud experience, toxic relationships and suspicious transactional patterns, behaviours and relationships.
19	Performance Objectives specific to fraud prevention and detection are in place for some staff.	We understand that anti-fraud management does not explicitly form part of the States objective setting or performance appraisal process.	We understand no change has been made since August 2012.	A competency framework for civil servants is currently being drafted.	**Objectives specific to anti-fraud management should be included in the performance management process of those States staff key to the implementation of the AFGF.**
20	Fraud response plan	The Fraud Guideline did include some high level	We understand no change has been	We understand that a formal fraud	**A formal fraud response plan should be**

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
	A formal fraud response plan has been established and approved by executive management. The plan is specific to the organisation and includes information such as who is responsible for investigating suspected fraudulent activity, what is the hierarchy for escalating fraud related issues, how will the investigation be conducted and who will pay for the investigation. Adequate and clearly defined responsibility for the external reporting of fraud to the Police and other relevant third parties (e.g. insurers) is included in the fraud response plan.	guidance to senior management on the procedures to be adopted if fraud or any other irregularity was detected or suspected. However this guidance was limited, with many key steps and issues omitted. The Fraud Rule included some elements of a Fraud Response Plan.	made since the August 2012.	response plan is being developed as part of the fraud improvement work package. The Fraud Rule is also being reviewed as part of the October 2012 States' Fraud Risk Management Improvement Plan.	**implemented.** Relevant staff should receive training on the fraud response plan. The plan should be tested. The States should ensure it has adequate resources to implement the plan, should an incident arise. The main components of a fraud response plan include: ► Triage of suspicions or Whistleblowing reports; ► Incident response and escalation; ► Roles and responsibilities of response team; ► Actions to be taken immediately following detection;

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
					► Identifying and securing evidence in a manner that will ensure it is legally admissible; ► Consideration of when to bring in subject matter experts, such as Law Officers, forensic technology experts etc; ► How to deal with employees who may be under suspicion, in line with other policies such as disciplinary; ► How to deal with third parties who may be under suspicion; ► Consideration of relevant local legislation (e.g. data protection etc); ► Ensure appropriate sanctions (disciplinary, civil, criminal) and redress (a clear policy on the

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
					recovery of any losses incurred and approach to, and monitoring of, the recovery of those losses); ► Informing insurers, as appropriate; ► Consideration of what lessons learnt and sharing as appropriate; ► Communication with staff and media; and ► Reporting and review.
21	Fraud investigation Policy, procedures and standards for the performance of an investigation in accordance with legal requirements and in line with leading practice. This should include a defined standard investigation methodology and reporting templates.	Per point 20 above, the Fraud Guideline did include some limited, high level guidance to senior management on the procedures to be adopted if fraud or any other irregularity was detected or suspected. While some individual Departments have	We understand no change has been made since August 2012.	Once the corporate fraud lead is identified, the October 2012 States' Fraud Risk Management Improvement Plan requires them to develop an annual performance survey of investigations conducted across the	**Policy, procedures and standards to support the States in the completion of effective investigations should be produced.** They should operate in accordance with the specific requirements of the fraud response plan e.g. the fraud response

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		investigation guidance, there was no specific, corporate fraud investigation policy, procedure or standards. There was no defined standard investigation methodology or reporting template. If investigating fraud incidents, the IAU would apply Internal Audit policy, procedures and standards.		States to develop an understanding of investigation efficiency and share good practice.	plan will stipulate who is authorised to undertake investigations, and these guidelines will then support those individuals in executing their role as investigator. The policy, procedures and standards will support authorised investigators but will not seek to remove appropriate management discretion or implement a 'tick box' investigation procedure. They will address issues such as: ► Key investigation steps – including triage of incidents or allegations and assessment of lessons learned; ► Minimum documentation requirements; ► Protecting the chain of evidence and related

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
					procedures; ► Handling of electronic evidence; and ► Interview procedures (including certain mandatory requirement such as the right to representation in line with related HR policies and procedures).
22	Adequately skilled resources Personnel are adequately skilled to perform their roles in relation to fraud investigation, skills gaps have been identified and development plans are in place.	We understand that the States has no central, dedicated anti-fraud resource. We note that some Departments have experienced investigation resources (for example Income Tax and Social Security). The Law Officers Department has historically been approached to provide legal advice on some	We understand no change has been made since August 2012.	We are not aware of any further planned actions.	**The existing investigation skills and capability within the States should be evaluated, with a view to bringing that resource under the control of the corporate fraud lead.** This will support the timely staffing of investigation teams with appropriately skilled personnel from across the business. The fraud response plan should include mandatory

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		investigations.			notifications of all investigations to corporate fraud lead.
23	Fraud investigation – computer forensics The fraud response plan includes agreed process to invoke a computer forensic examination to support investigation work.	The Fraud Guideline did refer to the need to secure all relevant documentation, including information on computer systems, discs, tapes etc. However there is no guidance on how this evidence should be secured, on first responder protocols or the process for invocation of computer forensic examinations. We understand that if computer forensics support were required, the States Police would have been approached for support.	We understand no change has been made since the August 2012.	We understand that a formal fraud response plan, which is currently being drafted as part of the fraud improvement work package, will include consideration of the requirement for investigations to be supported by computer forensics.	**The corporate fraud lead, and any other individuals tasked with fraud investigation within the States, should complete first responder training.** This training will help ensure that electronic evidence is not compromised at the commencement of, or during, an investigation.
24	Case management Basic case management system in place to support handling of alerts and resolution of	There was no central fraud investigation or alert case management	We understand no change has been made since August	We are not aware of any further planned actions.	**A basic case management system should be introduced.**

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
	cases	system.	2012.		This would ensure the application of consistent and appropriate investigation procedures. Such a system would record details including: ► Unique case number; ► Completion of mandatory steps/ minimum documentation requirements e.g. notification of insurers; ► Recording of key milestone dates e.g. disciplinary procedure timelines ► Identification of investigating team; ► Repository for investigation documentation or reference to where such documentation is held; and ► Summary of control

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
					weaknesses identified/ lessons learned.
25	Fraud intelligence Publicised high profile fraud cases are examined to establish if the organisation is vulnerable to similar incidents, and what learning can be brought back to strengthen existing control environment. Established relationships within the fraud prevention and investigation community, both locally and in similar organisations, to share (as appropriate) fraud experience and intelligence.	We understand that there was limited identification, review and communication of fraud intelligence pre May 2012. We note that an e-mail was received by the External Affairs team on 10 November 2011 which included a link to a BBC website article. The article noted that "criminals from the UK and overseas have sent legitimate-looking letters ... to persuade officials to change account details and redirect payments to them." The email was then forwarded, via the Director of Procurement, to the SAP Support team and Director of Client Services on the 11 November 2011. We understand that the	We understand no change has been made since August 2012.	We understand that the corporate fraud lead will be expected to collate and share information on high profile fraud cases.	**The corporate fraud lead should review high profile fraud cases and communicate lessons learned which could be applied to the States.** They should be alert to key fraud events occurring in similar organisations and the wider corporate environment. The corporate fraud lead should consider the applicability of the fraud method and fraud indicators to the States and communicate them as applicable. Communication of these messages should form part of the ongoing anti-fraud awareness training and communications programme, and utilise existing channels of

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		IAU monitored the activity of bodies such as the UK National Fraud Authority and had liaised with local law enforcement counter fraud and IT forensics points of contact. States employees who are members of professional accountancy and management bodies receive regular news, trends and updates from their professional bodies. Some of these cover fraud matters.			communication. **The corporate fraud lead should establish relationships with the fraud prevention and investigation community, both locally and in similar organisations.** This will help ensure that the States is aware of new fraud schemes more quickly and therefore able to respond more rapidly.
26	Fraud response – lessons learned Process in place to identify and disseminate lessons learned post investigation	We understand that there were no specific fraud response processes in place to identify and disseminate lessons learnt post fraud investigations. We understand that controls were updated after some fraud investigations, but this was more on an ad-hoc, reactive basis rather than as a result of a detailed	We understand no change has been made since August 2012.	We understand a fraud response plan is currently being drafted as part of the fraud improvement work package.	**The fraud response plan should include a process to identify and disseminate lessons learned post investigation.** This should, where relevant, include the updating of policies and procedures across the States.

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		fraud response plan step.			
27	Whistleblowing procedures The means for individuals to raise concerns through a dedicated confidential communication channel i.e. Whistleblowing hotline. The existence of the hotline is appropriately communicated to staff on an ongoing basis. Methods of communication may include (but are not limited to) induction training, anti-fraud training and awareness, relevant policies, internal publications, intranet. As part of the communications regarding the hotline, individuals are informed how a concern will be dealt with, to include: ► What happens if suspicions are wrong; ► How malicious calls are dealt with; ► How anonymous calls are dealt with; and ► How confidentiality of the whistleblower is ensured.	The Fraud Rule advises that an employee who suspects fraud is occurring, or that there may exist a high potential risk of fraud, should report their concerns immediately to the Chief Accountant and the Head of Internal Audit. In contrast the Fraud Guideline advises that an employee should bring their concerns to the attention of their immediate line manager, if their line manager is implicated, to the Chief Officer or the most senior officer available. If the Chief Officer is implicated, the Fraud Guideline notes that the employee should report their concerns to the Chief Internal Auditor or the States Treasurer. Neither the Fraud Rule not the Fraud Guideline provided detailed	We understand no change has been made since August 2012.	We understand a Raising Concerns at Work policy is currently being developed.	**A clear whistleblowing policy should be established, including how to make reports and how the reports will be dealt with, and communicated to staff on an ongoing basis.** A clear process should be in place and adhered to when responding to communication received. This process should consider the protection afforded to the individuals wishing to remain anonymous e.g. the support which the States will afford staff who have raised a concern where their anonymity cannot be maintained (i.e. where legal action has been taken and court procedures commenced) and should be consistent with the fraud response plan and related

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		information on how concerns would be dealt with.			procedures. Whistleblowing reports should be analysed to identify trends that could prevent further fraud or indicate potential control weaknesses.
28	Management information Management information relating to actual fraud, 'near misses' is centrally collated and reviewed for trends. The management information and any identified trends are circulated on a regular basis to executive management and other relevant parties.	We understand that there was no central collation or review of management information relating to fraud experience or 'near misses'. Inconsistent and unclear incident reporting lines have limited the ability to centrally gather or share fraud management information. We understand that information was shared between some Departments with respect to their relevant anti-fraud activity, for example in relation to the prevention of benefit or rent rebate fraud. However this information is not centrally	We understand no action has been taken since August 2012.	Fraud experience will be referred to in the Annual Report of the Head of Assurance. We understand that it is intended that the corporate fraud lead, once appointed, will collect and collate information from relevant internal officers with a role in anti-fraud activity. This is expected to enable reporting and allow more informed messaging should trends emerge.	**The corporate fraud lead should centrally collate, review and circulate fraud related management information.** The corporate fraud lead should combine this fraud related management information with fraud intelligence (see point 25 above) and whistleblowing reports (see point 27 above) to identify trends and should ensure that action is taken where necessary to address these trends. This will be facilitated by a single reporting line for all fraud allegations.

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
		collated.			
29	Key performance indicators Fraud related key performance indicators are established and subject to regular review.	We understand that there were no central, fraud related key performance indicators.	We understand no action has been taken since August 2012.	We are not aware of any further planned actions.	**Fraud related key performance indicators should be established and included as part of the management information described at point 28 above.**
30	Due diligence Staff and suppliers are subject to proper checks with regard to fraud risk. Due diligence includes open source background checks, where risk criteria deem necessary.	There is guidance available on conducting police checks on States recruits. We understand that it was the responsibility of the employing Department to make a risk based decision on the applicability of that guidance to each role. We understand that Procurement obtain financial information or review the accounts of tendering companies.	We understand no action has been taken since August 2012.	We are not aware of any further planned actions.	**The corporate fraud lead should conduct fraud risk due diligence on any roles or procurement designated as high risk.** **Consideration should be given as to whether the States need to revisit the due diligence on existing relationships or employees.**
31	Anti-fraud culture There is a culture of ownership of fraud awareness, detection and prevention by staff	We have been told that the culture was generally very trusting and naive with regard to fraud risk.	The July 2012 alleged mandate fraud incident has put the spotlight firmly on	The successful completion and embedding of the further planned actions detailed in	**The Executive Leadership Team should closely monitor the anti-fraud culture across the States to ensure it is**

Ref	Baseline expectation	Pre May 2012	Post August 2012	Further Planned Actions	Recommendations
	across the organisation. Staff take responsibility for their actions and are comfortable raising concerns. Anti-fraud is seen as the responsibility of all. Compliance with key policies and procedures is not considered optional.		fraud risk.	the October 2012 States' Fraud Risk Management Improvement Plan are expected to positively impact the anti-fraud culture across the States.	**sufficiently robust and allows staff to raise relevant concerns, yet does not tie the States in cumbersome 'red tape'. This should be considered as part of the rollout of the corporate approach to general risk management.**

Appendix E Ernst & Young anti-fraud maturity model

Anti-fraud factor		Starting (1)	Evolving (2)	Established (3)	Advanced (4)	Leading (5)
Anti-fraud governance		Anti-fraud strategy and supporting structure not in place. No clear tone from the top.	Anti-fraud strategy in place, but may not be formally documented and has not been communicated to staff. Clear tone from the top, but minimal communication to organisation.	Anti-fraud strategy had been established and approved by executive management. Anti-fraud roles defined and appropriate individuals assigned to roles. Clear tone from top, executive management demonstrate their involvement in anti-fraud management.	Anti-fraud strategy has been established, approved by executive management and communicated to relevant staff. Anti-fraud roles are clearly defined, and anti-fraud personnel are established within those roles. There is a clear and consistent tone from the top, regularly communicated and demonstrated by executive management.	Same as “Advanced” but includes anti-fraud strategy is well embedded into the overall organisational strategy; anti-fraud is part of ‘business as normal activities’.
Setting the proper tone	Code of ethics	Code of ethics has not been established.	Code of ethics has been created but has not been reviewed or approved by executive management.	Code of ethics has been established and approved by executive management. However the code is “boiler plate” in nature and is not specific to the organisation’s needs or desired tone.	Code of ethics has been established and approved by executive management. Additionally, the code is specific to the organisation and promotes honest and ethical conduct, full, fair accurate, timely and understandable disclosure in reports and documents; compliance with applicable governmental laws and regulations; prompt internal reporting of violations of the code; and accountability for adherence to the code and the sanctions to be imposed if the code is not followed.	Same as “Advanced”, but includes the effective communication of the code of ethics to new employees during their induction process, existing employees through annual confirmation process, and to significant contractors, partners and suppliers during the contractual process.

Anti-fraud factor		Starting (1)	Evolving (2)	Established (3)	Advanced (4)	Leading (5)
Setting the proper tone	Anti-fraud policies	Anti-fraud policies have not been established.	Anti-fraud policies have been established, but not approved by executive management.	Anti-fraud policies have been established and approved by executive management. However, the policies are "boiler plate" in nature and are not specific to the organisation.	Anti-fraud policies have been established and approved by executive management. Additionally, the policies are specific to the organisation and provide guidance for employees through complex issues, procedures that govern escalation of fraud allegations, and support / protection for whistleblowers.	Same as "Advanced", but includes the effective communication and access to the fraud policies to employees.
	Anti-fraud awareness training and communication	Fraud awareness training and communication programme has not been created.	Fraud awareness training and communication plan has been created, but it is not periodically reviewed by employees (i.e., training is only conducted during induction process) and is "boiler plate" in nature. Communication plan does not address the need for ongoing communication through a variety of channels.	Fraud awareness training has been created and is periodically reviewed by employees. Additionally, the training focuses on the organisation's code of ethics and protocols for reporting suspicious activities. Fraud awareness training forms part of the wider anti-fraud communications programme, which utilises various channels to raise staff awareness regarding anti-fraud. Communication is limited to pockets of staff, and is not embedded into standard business processes.	Fraud awareness training has been created and is periodically reviewed by employees. Additionally, the training focuses on the organisation's code of ethics, protocols for reporting suspicious activities, and disciplinary actions that may be taken in the event of fraud. The training illustrates examples of fraud schemes that may be common within the organisation (e.g. employee reimbursement schemes etc.) and red flags employers should be aware of regarding such schemes. Fraud awareness training forms part of the wider anti-fraud communications plan, utilising various channels to raise all staff awareness regarding anti-fraud.	Same as "Advanced", but includes the communication of training to significant contractors, partners and suppliers, and specific tailored training is offered to staff in areas which are more susceptible to fraud.

Anti-fraud factor		Starting (1)	Evolving (2)	Established (3)	Advanced (4)	Leading (5)
Proactive	Fraud risk assessment	A fraud risk assessment had not been conducted.	A limited scope fraud risk assessment (e.g. fraud risk assessment only conducted at specific location, fraud type – fraudulent statements, asset misappropriation, or corruption) has been conducted and the results communicated to executive management.	A stand alone fraud risk assessment has been conducted for the organisation and the results have been communicated to executive management.	A fraud risk assessment has been performed for the entire organisation and focused on fraud schemes that are common to most organisations, specific to the organisation. The results are communicated to executive management.	Fraud risk assessment is incorporated into the organisation wide risk assessment process.
	Controls monitoring	The indication and linkage of controls to mitigate fraud risks has not been performed.	Internal controls are linked to fraud risks indentified during the fraud risk assessment. However, no testing of the controls has been performed.	Internal controls are linked to fraud risks indentified during the fraud risk assessment. Additionally, testing the effectiveness of the controls has been performed.	Internal controls are linked to fraud risks identified during the fraud risk assessment. Additionally, a rationalisation and optimisation review is conducted to determine the most effective designed of controls (i.e. leveraging the IT general and application controls) to mitigate the fraud risks. The optimised internal controls are then tested to determine their effectiveness.	Same as “Advanced”, but includes the use of data analytics to indentify “red flags” in the organisation’s transactions that may indicate fraudulent activity.

Anti-fraud factor		Starting (1)	Evolving (2)	Established (3)	Advanced (4)	Leading (5)
Reactive	Fraud response plan	A formal fraud response plan has not been established.	A formal fraud response plan has been created and reviewed/approved by executive management. However, it is “boiler plate” in nature and not specific to the organisation.	A formal fraud response plan has been established and approved by executive management. The plan is specific to the organisation, but lacks information such a who is responsible for investigating suspected fraudulent activity, what is the reporting hierarchy for escalating fraud related issues, how will the investigation be conducted, who will pay for the investigation or how will monies be recovered, etc.	A formal fraud response plan has been established and approved by executive management. The plan is specific to the organisation and includes information such as who is responsible for investigating suspected fraudulent activity, what is the hierarchy for escalating fraud related issues, how will the investigation be conducted, who will pay for the investigation and how will monies be recovered, etc.	Same as “Advanced”, but included a uniform disciplinary procedures once a fraud is confirmed.

Ernst & Young LLP

Assurance | Tax | Transaction | Advisory

www.ey.com/uk