



PUBLIC ACCOUNTS COMMITTEE
THE STATES OF GUERNSEY

**REVIEW OF THE IMPACT OF THE
IMPLEMENTATION OF THE SAP SYSTEM
ON THE STATES OF GUERNSEY'S
FINANCIAL CONTROLS**

JULY 2015

CONTENTS

1. Chairman's Statement
2. Executive Summary
3. Background
4. The Review
5. Actions Taken Post Review
6. Recommendations

1. Chairman's Statement

In May 2013 when the Public Accounts Committee published its report on the anti-fraud governance framework in place in the States of Guernsey, it announced its intention to undertake a review of the financial control environment within the newly constituted Shared Transaction Service Centre (STSC).

This, the Committee's covering report, and the Ernst & Young report published alongside, is the culmination of that review.

The Committee is content with the overall findings and the response of the management of the Hub in giving prompt attention to implementing solutions to the defective controls that were highlighted during the Review.

However, the Committee has serious concerns that the States of Guernsey lacks a current, documented, comprehensive set of universal financial rules and directives. In the Committee's opinion, this should be implemented in any organisation without question, to assist in reducing the risk of fraud against it.

The Committee will be monitoring the situation to ensure that this is rectified with some expediency.



Deputy Heidi Soulsby
Chairman, Public Accounts Committee

2. Executive Summary

- 2.1. In July 2012, the States of Guernsey were defrauded of £2.6 million. As a result of this event, the Committee has undertaken a review programme intended to reduce the probability that such an incident would be repeated. This report represents the second stage of that review programme¹.
- 2.2. Following Stage One of the review in May 2013, the Committee stated that at the time of the occurrence of major fraud in July 2012, financial controls were weak and the concept of risk management was poorly understood. It also noted that the incident of fraud had been a catalyst for change and it was acknowledged that a significant amount of work had been undertaken following the incident to implement improvements. However, the Committee made it clear that momentum needed to be maintained.
- 2.3. The implementation of the SAP system and the creation of the Shared Transaction Service Centre (STSC) formed part of the Financial Transformation Programme and was designed to centralise and streamline the back office functions. The Committee therefore felt that it was necessary to determine whether these changes resulted, not only in financial control arrangements which were fit for purpose, but also whether continuous improvement could be demonstrated.
- 2.4. Ernst & Young was engaged on behalf of the Committee, to undertake the review of financial controls in place within this environment. The review was to look specifically at the quality of the financial management control systems in place in relation to reducing the risk of fraud.
- 2.5. In summary, the report provides a reasonable degree of assurance that a good standard of financial control is now in place within the STSC and those processes have indeed reduced the risk of fraud across the States.
- 2.6. However, it did highlight two matters of serious concern.
- 2.7. Firstly, the lack of a current, documented and comprehensive set of financial rules and directives. This should have been in place customarily, but more importantly, should have been a specific requirement prior to The Hub going live.
- 2.8. Secondly, it currently seems unclear who has overall responsibility for the financial management activities undertaken within the STSC.
- 2.9. In the Committee's opinion, the review also highlighted issues in terms of training within States departments, which may have resulted in the full benefits of the system not being realised at implementation. This should be considered as part of any future review into the SAP/STSC implementation.

¹ Public Accounts Committee Broad Review Terms of Reference: <http://www.gov.gg/CHttpHandler.ashx?id=77701&p=0>

3. Background

- 3.1. In September 2012, the Committee published its Terms of Reference² for a broad review of the effectiveness of financial controls in place across the States of Guernsey to minimise the risk of fraud against the organisation and safeguard States' assets.
- 3.2. It was agreed that the review would take a staged approach and, in November 2012, Ernst & Young was announced as the independent expert reviewer for the initial stage. This was to focus on the appropriateness of the States of Guernsey's anti-fraud governance framework before and after the specific incident of fraud committed against the States, which had been reported in July 2012.
- 3.3. In May 2013, both Ernst & Young's and the Committee's covering reports for this initial stage were released.
- 3.4. The Committee also announced at that time its intention that Stage Two of its 'Review of Financial Controls' would focus on the controls in place following the establishment of the STSC and the completed implementation of the new SAP system.

"As the implementation of both the STSC and SAP has had significant implications for financial management in the States of Guernsey, the Committee intends to commence Stage 2 of its Review of Financial Controls as soon as possible, focussing on the financial controls which are now in place."

- 3.5. The review was intended to evaluate the level of financial control being exercised within the States of Guernsey, the quality of the financial management control systems provided by the SAP system and the procedures undertaken by the STSC, in relation to reducing the risk of fraud.
- 3.6. Ernst & Young was engaged in late 2013 to undertake the review on behalf of the Committee.

² Public Accounts Committee Broad Review Terms of Reference: <http://www.gov.gg/CHttpHandler.ashx?id=77701&p=0>

4. The Review

- 4.1. Due to work commitments of the relevant sections of the Treasury and Resources Department throughout late 2013 and early 2014, Ernst & Young was unable to commence its fieldwork until July 2014.
- 4.2. Following completion of this initial work and the follow up undertaken in late 2014, Ernst & Young produced a draft report for consideration by the Committee. The Report entitled “Assessment of the Impact of SAP Implementation on the States of Guernsey’s Financial Controls” is attached as Appendix I to this report.
- 4.3. Ernst & Young’s review assessment was based on the current model of review³ of the States’ Internal Audit Unit, which concluded that the key financial controls in the accounts payable process of the States of Guernsey warranted a **Moderate Assurance** rating.
- 4.4. This is defined as;

“The strengths in risk management and internal controls outweigh weaknesses. Although there is a need for improvement in specific areas, the team, system, activity and/or process generally operate effectively”.
- 4.5. The Review as scoped, was broken down into three sections:
 - a) the key financial controls within the accounts payable processes;
 - b) certain elements of the Financial Management Governance Framework as they relate to the STSC and its role in mitigating fraud risk; and
 - c) the impact that the STSC has had on the financial control oversight provided by the Treasury & Resources Department.

Accounts Payable Processes

- 4.6. The reviewer identified twenty four accounts payable processes that fell within the scope of this particular review, within which one hundred and three controls were currently in place.
- 4.7. Following the Committee’s direction, sixty four of those controls were chosen to be tested. Subsequently, walk-throughs of all the processes were undertaken by Ernst & Young to enable it to understand each process and to be able to identify any risks of fraud.
- 4.8. In the course of the review, nine of the controls were deemed to be ineffective during the initial testing phase prior to the end of September 2014. Following further investigation and feedback to the STSC, the majority of these issues were resolved and just three controls were still deemed to be ineffective during subsequent testing undertaken in late 2014.
- 4.9. The Department should be commended in terms of how quickly the corrections were made to the majority of the defective controls once identified, highlighting the experience and capabilities of the staff within the STSC.

³ The States of Guernsey’s Internal Audit Model of Review can be found at Appendix 2

- 4.10. However, Ernst & Young believes that without full support from the Departments outside the STSC in following the overall procurement processes, the risk of fraud across the States of Guernsey could increase.
- 4.11. At the time of the review, purchase order (PO) compliance measured as a percentage of total number of purchases, was performing at or above the set target level. Unfortunately, the average PO compliance measured as the percentage of total spend derived from purchase orders, was performing below the set target level.
- 4.12. Ernst & Young concluded that an extensive programme of training had been carried out prior and post the launch of the STSC. However, the underperformance in PO compliance brings into question the effectiveness of the training roll out throughout the States.
- 4.13. The level of training being provided should be considered as part of any future review into the SAP/STSC implementation.

Elements of the Financial Management Governance Framework as they relate to the STSC and its role in mitigating fraud risk

- 4.14. This section of the review took into consideration the current mandatory Financial Rules and Directives as they relate to the STSC and their role in fraud risk reduction.
- 4.15. The work undertaken by Ernst & Young highlighted a matter of serious concern in that the States of Guernsey does not have a documented, comprehensive set of Financial Regulations. The latest Financial Rules and Directives were issued more than five years ago.
- 4.16. The report also highlighted the lack of a comprehensive documented procedure covering all aspects of the 'procure-to-pay' process, prior to the launch of the new system in January 2013.
- 4.17. It is disappointing that neither of the above were deemed to be specific requirements prior to the STSC going live, especially as the external auditors to the States have previously highlighted this issue in their audit summary report.

The impact that the STSC has had on the financial control oversight provided by the Treasury & Resources Department

- 4.18. The Committee understands that prior to the STSC going live, a re-structuring of senior roles occurred within the Treasury and Resources Department. The position of States Treasurer was re-introduced with the associated responsibility for all financial matters. In addition a role of States Chief Corporate Resources Officer was created with responsibilities, amongst many other things, for the performance of the STSC.
- 4.19. Ernst & Young have highlighted that, despite the States Treasurer having responsibility for all financial matters, at the time of review she was not in receipt of the monthly Key Performance Indicators (KPIs). However the States Chief Corporate Resources Officer had received this information since the STSC's go live date of January 2013.

- 4.20. The review also found that some of the key KPIs that the STSC uses to monitor compliance with procurement processes had plateaued, and in some cases had deteriorated. In these circumstances this information should have been provided to the States Treasurer.
- 4.21. Although the Committee understands that this issue was in the process of being addressed at the culmination of the review, it highlights a potential lack of clarity in overall responsibility for the financial management activities undertaken within the STSC.
- 4.22. The Committee believes that the Treasury and Resources function would benefit from a clear statement on the responsibilities allocated for financial matters within the STSC.

5. Actions Taken Post Review

- 5.1. Upon conclusion of the Review, the PAC provided Ernst & Young's draft report to the Treasury and Resources Department for comment and an update on the three outstanding defective controls.
- 5.2. After review, the Treasury and Resources Department confirmed to the Committee that two of the three Ernst & Young recommendations could not be technically implemented as written. However, alternative methods of working had been implemented which effectively delivered the recommendations. The third was in the process of being addressed by the supplier.

6. Recommendations

- 6.1. The States Treasurer should ensure that the Financial Rules and Directives of the States of Guernsey are updated without delay and a comprehensive set of Financial Regulations covering all relevant elements of managing the States' financial affairs is circulated forthwith.
- 6.2. The States Chief Corporate Resources Officer should continue to closely monitor Purchase Order compliance to ensure that the organisation is performing at, or above, the set target level.
- 6.3. The States Chief Corporate Resources Officer and States Treasurer must ensure that relevant training is provided to all parts of government to ensure effective financial control.
- 6.4. The Committee believes that the Treasury and Resources function would benefit from a clear statement on the responsibilities allocated for overall financial management within the STSC.

Assessment of the Impact of SAP Implementation on the States of Guernsey's financial controls





Ernst & Young LLP
Royal Chambers
St Julian's Avenue
St Peter Port
Guernsey
GY1 4AF

Tel: 01481 717 400
Fax: 01481 713 901
www.ey.com/channel_islands



Privileged 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 January 2015

Our ref: DRJM

Tel: +44 (0)1534 288697

Email: dmoore@uk.ey.com

Dear Deputy Soulsby

We have completed our engagement to assess the impact of the SAP implementation on the States of Guernsey's financial controls.

Our engagement was performed in accordance with our engagement agreement dated 17 March 2014, extracts of which are set out in Appendix A. Our procedures were limited to those described in that agreement.

During the period from mid-July 2014 to mid-October 2014, EY assessed:

- a. the key financial controls within the accounts payable processes;
- b. certain elements of your Financial Management Governance Framework as they relate to the Shared Transaction Services Centre and its role in mitigating fraud risk; and
- c. the impact that the Shared Transaction Services Centre has had on the financial control oversight provided by the Treasury & Resources ('T&R') department.

Our findings resulting from our work are provided within this report.

Limitations on scope

Our work consisted of analytical procedures applied to information and data made available to us, and explanations provided to us. Our procedures did not intend, or seek, to express an audit opinion on the information and, therefore, do not constitute an audit and should not be relied on as such. Our work has been limited in scope and time and we stress that more detailed procedures may reveal issues that this engagement has not. None of the Services or our report constitutes any legal opinion or advice.

Assessment criteria

As agreed with you, the following assessment criteria used by your Internal Audit Department were utilised in our assessments:

- a) Full Assurance: Risk management and internal control activity is sufficient to secure the consistent and effective achievement of the objectives of the team, system, activity and/or process. The impact of any non-compliance with key controls is low.
- b) Moderate Assurance: Strengths in risk management and internal control outweigh weaknesses. Although there is a need for improvement in specific areas, the team, system, activity and/or process generally operate effectively.



- c) Partial Assurance: There is a risk to the achievement of the objectives of the team, system, activity and/or process. Some of the key controls are either missing or not operating effectively.
- d) No Assurance: Control is insufficient to secure the consistent achievement of the objectives of the team, system, activity and/or process. Many of the key controls are either missing or not operating effectively.

The criteria do not represent any conclusion as to the effectiveness or adequacy of your internal financial controls and related processes. Only you can assess whether the controls, functions, processes or programs you have implemented are adequate to meet your objectives.

Limitation of liability

We draw your attention to section 6 of the "Agreement for provision of value for money reviews to the States of Guernsey" which refers to the limitation of this firm's liability.

This Report was prepared on your specific instruction solely for the purpose of this engagement and should not be relied upon for other purpose. 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 it entirely at their risk.

Finally, we appreciate the cooperation and assistance provided to us during the course of our work. If you have any questions, please do not hesitate to contact me.

Yours sincerely

A handwritten signature in black ink, appearing to be 'DM', is located below the 'Yours sincerely' text.

David Moore
Partner
Ernst & Young LLP

Abbreviation	Definition
States/SoG	States of Guernsey
PAC	Public Accounts Committee
EY	Ernst & Young LLP
STSC/HUB/Hub	Share Transactions Services Centre
FAC	Financials Audit Controls
KPIs	Key Performance Indicators
WCGW	What can go wrong - A risk within a process that has a likelihood of occurrence and magnitude that could result in a material misstatement
Walk-through	A procedure undertaken to confirm our understanding of a process
PO	Purchase Order
CUA	Centralized User Access Management tool
Financial Regulations	Provide the framework/policy/responsibilities for managing the financial affairs of an organisation
Application controls	Application controls are automated controls processed by the organisation's Information Technology ('IT') applications without input from a person and relate to procedures used in the critical path of transactions or other financial data. Application controls help ensure that transactions are authorized, and are completely and accurately recorded and processed. Application controls can be classified as edit checks, validations, calculations, interfaces and authorizations
Manuals controls	Manuals controls are performed by individuals typically outside of a system. Examples of manual controls could be a supervisor review or sign-off of a document.
ERS	Evaluated Receipt Settlement
SAP roles	SAP Roles are defined as collections of certain activities used in different business scenarios. In the normal course of business each user is assigned to certain activities and restricted to others to ensure that business data is secure. To complete these assigned activities users can access SAP functions (T/t-Codes) to perform their day to day activities.
SAP Standard Role	<p>SAP Standard Roles can be built-into SAP roles, and hence the latter are more tailored.</p> <p>(Please note that we have been told that the States do not use SAP Standard Roles, hence we excluded those from our analysis)</p>

Abbreviation	Definition
Composite Role	A single role is a collection of t-codes and/or authorization objects, whereas a composite role is a role that contains a number of single roles. Composite roles are used to easily manage users with roles in different SAP modules.
Derived Role	Single – Derived Role concept is used when SAP is used in different locations and level authorisation remains the same across all sites.
T – Code	T-codes are the functions that a user applies in a day-to-day activity; each function has a T-code assigned to it.
SAP Supplier Relationship Management ('SRM'/'SAP SRM')	SAP SRM is a module that allows an organisation to manage its relationships with its vendors.
SAP ERP Central Component ('SAP ECC')	<p>The previous SAP R/3 product name has been changed to SAP ECC, the latest version being the ERP ECC 6.0.</p> <p>SAP ECC is a generic term for all functional modules, of which SAP SRM is one.</p>

Contents

Executive summary 2

Assessment of key financial controls within the accounts payable processes 5

Assessment of elements of your Financial Management Governance Framework as they relate to the STSC and its role in fraud risk reduction..... 9

Assessment of the impact that the STSC has had on the financial control oversight provided by the Treasury & Resources ('T&R') department..... 11

Executive summary

Background

1. In 2009 the Financial Transformation Programme ('FTP') commenced with the aim of driving efficiencies and reducing costs across the States of Guernsey ('the States/SoG'). We understand that as part of the Financial Transformation Programme the existing SAP solution was re-developed and enhanced to deliver, inter alia, greater efficiency, cost savings and improved management information across the States. A shared services model was also adopted in tandem with this enhancement and the 'Shared Transactional Services Centre' ('STSC/HUB/Hub') created.
2. The Hub provides support to all States Departments for their common corporate business processes with the aim of driving consistency and efficiency of operations. Examples of Hub services include payroll, recruitment, cashiering, IT support and accounts payable management.
3. The revised SAP solution includes Finance & Procurement functionality and we understand that a centralised approach is now provided across many financial transactional activities, including the accounts payable processes.

Purpose of Review

4. As a result of the changes noted above, the Public Accounts Committee ('PAC/you') engaged us to perform an independent assessment of specific areas of the States financial control environment affected by the SAP implementation on the States' Financial Controls.

Scope of services

5. In summary, our engagement focused on an assessment of:
 - a. the key financial controls within the accounts payable processes;
 - b. certain elements of your Financial Management Governance Framework as they relate to the STSC and its role in mitigating fraud risk; and
 - c. the impact that the STSC has had on the financial control oversight provided by the Treasury & Resources ('T&R') department.
6. Our detailed scope of our services is set out in Appendix A of this report.
7. Our assessment was based upon analysis of documentation received from you and the Hub, enquiries of States personnel, walk-throughs of accounts payable processes and limited testing of those controls in the accounts payable processes deemed key by yourselves.

Assessment criteria and findings

8. As agreed with the PAC, the following assessment criteria used by the States Internal Audit Department were utilised in our assessment:

Full Assurance: Risk management and internal control activity is sufficient to secure the consistent and effective achievement of the objectives of the team, system, activity and/or process. The impact of any non-compliance with key controls is low.

Moderate Assurance: Strengths in risk management and internal control outweigh weaknesses. Although there is a need for improvement in specific areas, the team, system, activity and/or process generally operate effectively.

Partial Assurance: There is a risk to the achievement of the objectives of the team, system, activity and/or process. Some of the key controls are either missing or not operating effectively.

No Assurance: Control is insufficient to secure the consistent achievement of the objectives of the team, system, activity and/or process. Many of the key controls are either missing or not operating effectively.

Summary findings and assurance statement

9. Across the 24 accounts payable processes in our scope, we identified 103 controls to mitigate WCGWs. Based on your direction; we tested 64 controls, of which 45 were application controls and 19 manual controls.
10. Of these, 9 were deemed ineffective at the point of testing, of which only 3 remained ineffective at the date of re-testing in October 2014.
11. Our analysis of the total of assigned/unassigned for normal, derived and composite roles in SAP SRM yielded the following:
 - a. Unassigned roles have been well managed;
 - b. As a percentage, and using the financial services sector as a comparison, we believe that the number of roles with more than 5 t-codes assigned to them appears high and may increase the risk of inappropriate segregation of duties were those specific t-codes to be incompatible; and
 - c. At the time of testing there were 4,809 identified users of SAP SRM. Of these, there were 2,376 inactive users of which we understand that 2,250 could be enabled to obtain access to SRM.
12. In our view, subject to the limitations outlined in this report, and utilising the assessment criteria used by your Internal Audit Department, we have assigned a **Moderate Assurance** rating to the key financial controls in the accounts payable processes.
13. *However*, without the support from the States Departments outside the HUB in following the overall procurement processes, the HUB becomes less efficient and, in our view this could increase the risk of fraud across the States.
14. We understand that extensive training and communication has been rolled out since early January 2013 to all States departments, but note with some interest that some of the Key Performance Indicators ('KPIs') that the HUB uses to monitor States department's compliance with procurement processes have plateaued, and in some cases have deteriorated recently.
15. In our view, this is unacceptable.
16. The States department's Chief Officers are ultimately responsible for ensuring that the internal control framework in place in their department is appropriate and the standards set are met regardless of whether part of a process or function has been delegated to another part of the States.
17. This includes, for example, challenging the finance services delivered by the co-located finance function, or indeed the HUB and its vendor services, if they believe they are inadequate; responsibility for out-sourced functions can only be delegated, not abdicated.
18. In our view, consideration should be given to this responsibility taking the form of a quarterly attestation by the Chief Officers; this would drive compliance with overall procurement processes and further reduce the risk of fraud.
19. This could be supported by an equivalent attestation, perhaps monthly in frequency, by the HUB's Central Services Director and provided to both the States Treasurer and States Chief Corporate Resources Officer on the control environment surrounding the processes and procedures that are within his remit.

20. A further roll-out of training by the HUB to other departmental staff would support this change, along with other changes, such as a regular independent monitoring procedure of SAP substitute roles to ensure authorisation levels are being followed.
21. The States neither have a current, comprehensive set of Financial Regulations nor a comprehensive documented procedure covering all aspects of 'procure-to-pay'. We realise that there are many demands on States resources, but this is unhelpful, and we urge those responsible to work towards updating all States Rules and Directives so there is no ambiguity, issuing a comprehensive, not piecemeal, set of Financial Regulations covering all relevant elements of managing the States financial affairs.
22. Finally, the HUB should be congratulated on their efforts and ongoing commitment over the last 2 years; based on our work, we consider that the processes they have put in place have reduced the risk of fraud across the States. However, to leverage the full benefit, it needs other departments to fully utilise them.

Assessment of key financial controls within the accounts payable processes

Methodology - general

23. In our letter of engagement dated 17 March 2014, you set out the accounts payable processes within the scope of this assignment.
24. As a result, in order to obtain an understanding of these processes, we:
 - a. Read documentation obtained from, and deemed relevant by you and relevant States departments, as set out in Appendix B;
 - b. Performed a subsequent desk-top analysis of that documentation; and
 - c. Made enquiries of relevant States personnel as defined by you.
25. Subsequently, we performed walk-throughs of all processes set out in Appendix C to confirm our understanding and to identify the risks of fraud or error within these processes. For the avoidance of doubt, and as agreed by you, the scope of our work did not include the processes around the execution of payments.
26. In our walkthroughs, we considered both the manual and automated steps of the processes, such as authorization, information processing and information technology application controls.
27. Our inquiries of States' personnel included follow-up questions about what they do when they encounter errors, the types of errors they have encountered, what happened as a result of finding errors and how the errors were resolved. This approach was adopted to help identify overrides of controls, or risks of material misstatement due to fraud. This enquiry was also performed in order for us to either confirm "what can go wrongs" ("WCGWs") already identified by the States' personnel or to identify other WCGWs that had not been identified before.
28. Across the 24 accounts payable processes we identified 103 controls to mitigate these WCGWs.
29. Having performed the above steps, we met with you to confirm which of these controls you considered to be key, based upon your desired level of financial control as communicated to us. As a result 64 controls were identified; 45 application controls and 19 manual controls. These are set out in detail in Appendix E.
30. The population from which the samples were selected for limited testing were limited to the month of June 2014 for transactions to test application controls, and from January to June 2014 for those manual controls.
31. We assumed that the population that we were given included all relevant items throughout the period. We have not performed specific tests to determine whether or not items have been omitted from the population.
32. We selected our sample of items for controls testing using a random selection methodology.
33. We tested one instance ('test of one') of each application control for each type of transaction and process. Where exceptions are identified we would expand our sample to 25.
34. We have not tested the SAP set-up and configuration, and have performed our tests on the assumption that the overall IT environment is effective, and hence supports the IT applications.
35. For manual controls that are performed daily or many times per day we tested 25 items. Where exceptions are identified we would expand our sample to 60.

36. Some of the procedures we used to obtain evidence when testing controls were:

a. Inquiries

- We sought information from knowledgeable persons, both in the HUB and other States departments. Inquiries were either in written or oral form.
- We evaluated their responses, as this sometimes provided information not previously obtained or corroborated by evidence already obtained.

b. Observation

- We observed processes or procedures being performed by the States' personnel. Observation provides evidence about the performance of a process or procedure, although it is limited to the particular point in time at which the observation takes place. In addition, the act of being observed may affect how the process or procedure is performed.

c. Inspection

- We examined records or documents, whether internal or external, in paper or electronic form. Inspection of records and documents provides evidence of varying degrees of reliability, depending on their nature and source and, in the case of internal records and documents, on the effectiveness of the controls over their production.

d. Re-performance

- We executed, sometimes in the testing environment and with the assistance of the State's personnel, the relevant controls that were originally performed as part of the entity's internal controls to obtain evidence that the control performed as designed.

Methodology – SAP specific

37. In addition, we performed analytics (as set out in paragraphs 43 and 44 below) on the SAP Supplier Relationship Management ('SRM'/'SAP SRM') module data set provided to us, specifically performing T-codes and users' analysis.

38. T-codes can be seen as the functions that a user may need to use in a day-to-day activity; each function has a T-code assigned to it. Example unique T-codes could be 1) the ability to create a purchase order, 2) the ability to authorise it, 3) the ability to create an invoice.

39. We were also informed that a Centralized User Access Management ('CUA') tool is used to create/amend/lock users. This acts as a gateway to the SAP Modules, such as SAP SRM.

40. We noted that when a user is created/amended/locked by CUA, changes will automatically be made into each SAP module. As a result, when there is the need to restrict a user's access to only one SAP module, this is not possible because the lock function is a centralized function and locking the account will result in limiting access to all SAP modules.

41. However, we understand that even though a user may be able to 'see' a specific SAP module, such as SRM, without the relevant approved functional access rights assigned to them they cannot perform any tasks in that module.

42. We were informed that SAP audit logs are kept for review and audit trail, hence inactive users are not deleted, but rather locked when deemed appropriate to do so by SAP support.

43. We analyzed the total of assigned/unassigned for normal, derived and composite roles as follows:

- a. Roles with t-codes assigned
 - b. T-codes assigned per role (Average)
 - c. % Roles with more than 5 t-codes assigned
 - d. % Roles with more than 100 t-codes assigned
44. In addition, we analyzed the total number of users with roles assigned and unassigned, and the total number of inactive users that have been inactive for more than 90 days and that have not been 'locked'
45. As all the IT controls tested in this assignment reside in the SAP SRM module, we focused our analysis on the SAP roles, T codes and users' analysis in the SAP SRM module; however, for completeness we have also analysed the users, roles and T code analysis in the ECC SAP module.
46. We completed the majority of our fieldwork in mid-July 2014 to early September 2014.
47. The scope of this assignment did not include a review of the appropriateness of the SAP SRM roles allocated to each of the 4,809 users on SAP SRM, but did include an analysis of the number of T-codes allocated to those users.
48. The allocation of roles and responsibilities, including unique T-codes and associated authorisation limits to ensure appropriate segregation of duties, is obviously a key part of the States' internal control framework and, although we have not tested it, we understand that SAP SRM roles have been allocated to users based on job functions per the original 'blueprint' design.
49. In our view, assisted by SAP support in the HUB, it is the responsibility of each States department's Chief Officer to have oversight of these allocations as they form an integral part of the internal controls of each department; with Senior Finance Officers, the Chief Officers are responsible for ensuring the development, implementation and maintenance of Fraud Risk Management (as defined in the Finance Directive:Fraud) is in line with corporate processes and procedures.

Findings

50. Based upon the work performed above, we have captured our detailed findings and recommendations in Appendices F and G.
51. In summary, of the 64 controls we tested, we identified 9 controls that we deemed were ineffective at the point of testing. For these ineffective controls our samples were extended as set out above.
52. We note that the HUB has resolved the majority of these issues quickly and, although outside the scope of our assignment, we have subsequently performed limited testing on those controls in early October to corroborate their assertions of rectification. At the date of re-testing only 3 of the 9 controls remained ineffective.
53. Our analysis of the total of assigned/unassigned for normal, derived and composite roles in SAP SRM yielded the following:
- a. Unassigned roles have been well managed;
 - b. As a percentage, the number of roles with more than 5 t-codes assigned to them appears high and may increase the risk of inappropriate segregation of duties were those specific t-codes to be incompatible. Without further detailed analysis, which is outside the scope of this assignment, it is not possible to conclude on their compatibility; and

- c. At the time of testing there were 4,809 identified users of SAP SRM. Of these there were 2,376 inactive users of which 2,250 have never logged into SAP SRM. In our view there is a heightened risk associated with potentially allowing nearly 50% of users access to SAP SRM when they have never logged into it and hence we assume do not need access to it. Ideally inactive and users without roles should be disabled or deleted, or if the CUA model does not practically allow this, additional risk monitoring processes should be considered. However, if a user has no SRM t-code roles assigned to their user account, we understand that it will not be possible for them to access SRM.

- 54. From the limited controls testing and SAP analysis set out above, we have assessed the key financial controls within the accounts payable processes.
- 55. In our view, subject to the limitations outlined above and utilising the assessment criteria used by your Internal Audit Department, we have assigned a **Moderate Assurance** rating to the key financial controls in the accounts payable processes.

Other observations

- 56. As part of our review we also obtained the HUB's key performance indicators ('KPIs') from January to June 2014. These KPIs take many forms and are more than 20 in total for the relevant processes in scope of this assignment.
- 57. We noted that across the 14 States departments the average purchase order ('PO') compliance measured as a percentage of total number of purchases derived from purchase orders is performing at or above the set target level, however the average PO compliance measured as the percentage of total spends (value) derived from purchase orders is performing below the set target level. This is set out further in Appendix H.
- 58. Over the first 6 month ends of the year, individual departmental compliance ranged from 98% to 20%; the latter is obviously unacceptable and we set out our views further in paragraphs 67-68 below.

Assessment of elements of your Financial Management Governance Framework as they relate to the STSC and its role in fraud risk reduction

59. Using your criteria in the context of your desired level of fraud risk reduction as communicated by you, and the output from the steps above, we assessed those elements of your current Financial Management Governance Framework, as set out below, as they relate to the STSC and its role in fraud risk reduction:
- a. The Rules and Directives as set out in Appendix B
 - b. Processes as outlined in Appendix C
 - c. The roles and responsibilities in the processes in b. above
60. By way of background, we understand that the States of Guernsey Rules and Directives for Financial and Resource Management are mandatory and should be followed by all States Personnel. Moreover, these mandatory Policy statements are supported by recommended Guidance on specific areas, and detailed processes and procedures created at the departmental level.
61. This framework also covers the acquisition, management and procurement of public funds and resources. As a result, the STSC/HUB can be seen as the embodiment of those mandatory rules around the procurement of goods, materials and services which arguably all States Departments should follow.
62. The HUB is responsible for the operation of its processes and procedures, which include a number outside of procurement. Furthermore, we understand that these processes and procedures were designed and are owned by HR, Finance and Procurement, and that the blueprint designs were approved by those departments; they were responsible for the design, whilst the HUB is responsible for the operation.
63. We identified that there were 4,809 users (2433 active users) in SRM at the date of our analysis, many with different functional roles. Given this, it has not been possible to analyse and conclude on the appropriateness of their allocated t-codes, and hence assigned roles and responsibilities in the processes outlined in Appendix C. However, Appendix G sets out our roles and transactions analysis.
64. Moreover, it is crucial to note that the procurement process both starts and finishes outside of the HUB, in the States Departments. Inter alia, the HUB is responsible for the payments made to States suppliers and we understand through discussions with management that controls are in place to ensure payments are made only when a full audit trail of documentation is in place, with the HUB processing over 100,000 invoices equivalent to more than £200m per year.
65. Without compliance with corporate processes by States Departments in following the overall procurement processes, the HUB becomes less efficient and, in our view, there is a heightened risk of fraud across the States.
66. We understand that extensive training and communication has been rolled out since early January 2013 to all States departments, but note with some interest that some of the Key Performance Indicators ('KPIs') that the HUB uses to monitor compliance with procurement processes have plateaued, and in some cases have deteriorated recently.
67. In our view, this is unacceptable. As noted above in paragraph 58, the States department's Chief Officers are ultimately responsible for ensuring that the internal control framework in place in their department is appropriate and the standards set are met regardless of whether part of a process or function has been delegated to another part of the States; part of the role of internal control is to minimise the risk of fraud occurring and they are ultimately responsible for ensuring that their

department is complying with the standards set around fraud risk, regardless of those delegated parts.

68. In our view, consideration should be given to this responsibility taking the form of a quarterly attestation by the Chief Officers; this would drive compliance with overall procurement processes and further reduce the risk of fraud. This could be supported by a further roll-out of training by the HUB to other departmental staff.
69. However, we understand that presently the States do not have a current, comprehensive set of Financial Regulations. For example, the Rules for Financial and Resource Management were issued in 2009 and, as a result, if a rule does not exist we understand that a user may need to refer to an even older, hard copy document for direction.
70. Moreover, we would expect a comprehensive documented procedure covering all aspects of 'procure-to-pay' to exist across the States; this would not only encapsulate the documented procedures in the HUB, but would also capture steps in the process outside the HUB, such as initiation.
71. We realise that there are many demands on States resources, but we urge those responsible to work towards updating all States Rules and Directives so there is no ambiguity, and issuing a comprehensive set of Financial Regulations that covers all relevant elements of managing the States financial affairs. These should be supported by updated detailed standards and, where appropriate, reference to other appropriate and updated guidance.
72. Finally, the HUB should be congratulated on their efforts and ongoing commitment over the last 2 years; based on our work, we consider that the processes they have put in place have reduced the risk of fraud across the States.

Assessment of the impact that the STSC has had on the financial control oversight provided by the Treasury & Resources ('T&R') department.

73. By way of background, during the last quarter of 2012 a re-structuring of roles occurred whereby the position of States Treasurer was re-introduced with the associated responsibility for all financial matters. In tandem with this appointment was the appointment of a States Chief Corporate Resources Officer with responsibilities, inter alia, for all non-financial resources including HR, property, IT and the performance of the STSC/HUB. We understand that the blueprint design for the processes and procedures within the STSC were approved by both individuals.
74. We understand that this split of roles was created because the States Treasurer sets the Rules and Directives for Financial and Resource Management and it was believed that there would be an inherent conflict if they were also responsible for its performance.
75. As a result, it was decided that the Central Services Director would be responsible for the day-to-day operations of the HUB and report directly to the States Chief Corporate Resources Officer who, we understand, is ultimately responsible for its performance.
76. However, given that the States Treasurer has responsibility for all financial matters and on a yearly basis there are approximately £200m of payments made to States suppliers through the HUB, we are surprised that the States Treasurer has not received at least a copy of the monthly KPIs that the States Chief Corporate Resources Officer receives since the HUB's operational commencement in January 2013. We understand that this is in the process of being addressed.
77. Although we have not reviewed or tested the related processes and controls, we understand that T&R control finances through regular accounts reconciliations, and management analytics and reporting. Moreover, although the HUB performs its own monitoring procedures, we understand T&R are in the process of recruiting a separate compliance officer to independently review the automated processes in the HUB.
78. Although we have not had sight of the review as it is outside the scope of our assignment, we understand that T&R have issued clear rules on the levels of authorisation based on seniority of staff that individual States Departments should follow, articulating that any deviation from those standards requires States Treasurer approval.
79. During our SAP testing of substitute approvers, we were furnished with a report which identified levels of staff seniority. As a result, we suggest consideration is given to creating a regular independent monitoring procedure to ensure authorisation levels are being followed.
80. We would also suggest that, similar to our consideration of a quarterly attestation by the Chief Officers, a monthly attestation by the Central Services Director should be provided to both the States Treasurer and States Chief Corporate Resources Officer on the control environment surrounding the processes and procedures that are within his remit.

Other observations

81. Moreover, recently the States has moved from having separate finance individuals in each States department supporting the department, to one central finance function whose team members are located in the individual States departments and provide finance services to the departments in which they are located.
82. Ultimately the Chief Officers are responsible for ensuring that the internal control framework in place in their department is appropriate. This includes challenging the finance services delivered by the co-located finance function, or indeed the HUB and its vendor services, if they believe they are inadequate; responsibility for out-sourced functions can only be delegated, not abdicated.