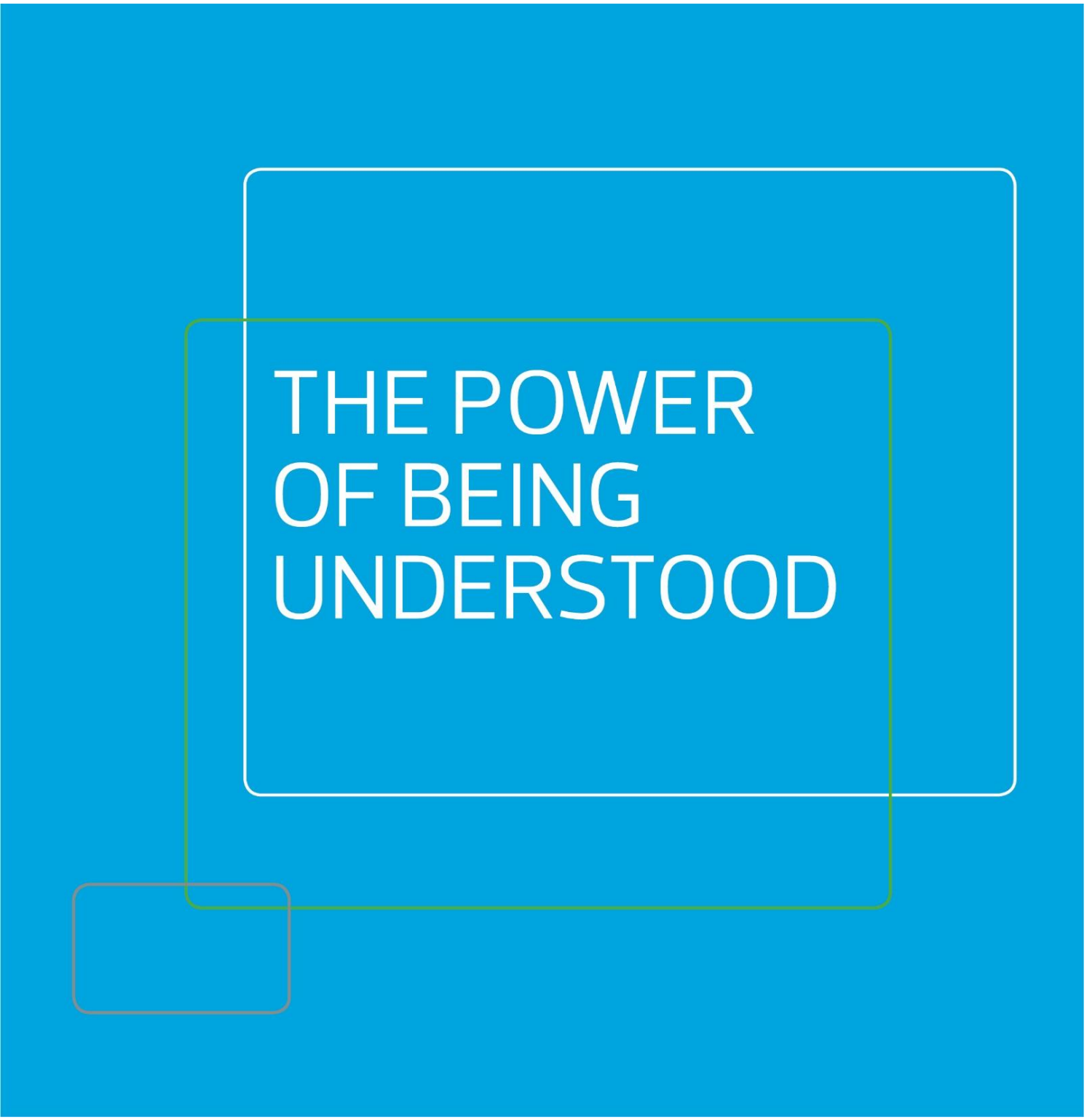

EPSOM AND EWELL BOROUGH COUNCIL

Internal Audit Progress Report

Audit, Crime & Disorder and Scrutiny Committee Meeting

26 November 2015

RSM

CONTENTS

As a practising member firm of the Institute of Chartered Accountants in England and Wales (ICAEW), we are subject to its ethical and other professional requirements which are detailed at http://www.icaew.com/en/members/regulations-standards-and-guidance.

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made.

Recommendations for improvements should be assessed by you for their full impact before they are implemented. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

This report is supplied on the understanding that it is solely for the use of the persons to whom it is addressed and for the purposes set out herein. Our work has been undertaken solely to prepare this report and state those matters that we have agreed to state to them. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any party other than the Board which obtains access to this report or a copy and chooses to rely on this report (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to our Client on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

1 INTRODUCTION

The Internal Audit Plan for 2015/16 was approved by the Committee in Date 9 April 2015. This report provides a summary update on progress against that plan and summarises the results of our work to date.

2 REPORTS CONSIDERED AT THIS AUDIT COMMITTEE

This table informs of the audit assignments that have been completed and the impacts of those findings since the last Audit Committee held.

The Executive Summary and Key Findings of the assignments below are attached to this progress report at Appendix A.

Assignment	Opinion issued	Actions agreed		
		H	M	L
Attendance (1.15/16)	Green	-	1	1
Recruitment (2.15/16)	Amber/Green	-	1	5
Review of Anti-fraud and Anti-bribery Arrangements (2013/14) (3.15/16)	Advisory	1	5	3
Cash Handling (4.15/16)	Amber/Green	1	3	2
Venues (5.15/16)	Amber/Green	-	1	1
Information Governance (6.15/16)	Amber/Green	-	2	8
PCI Compliance Control Framework (8.15/16)	Amber/Red	3	6	-

In addition we have completed our advisory review of CRM: Support Knowledge Transfer, and management have agreed to findings and are working on an action plan to take the matters raised forward.

2.1 Impact of findings to date

To date there are no areas that we need to bring to your attention as adversely impacting on our annual opinion.

Overall the level of findings and recommendations is low and management actions are being responded to in a timely manner.

2.2 Themes arising from our findings

The table below shows the issues we have flagged to date in our reports this year, and the underlying causes of the control weaknesses.

Root cause	High	Medium	Low
Policies and / or procedures out of date	1	6	4
Non-compliance with policies / procedures	-	3	1
Poor design of the control framework	3	5	5
Lack of training / awareness for staff	1	2	4
Lack of or poor management or performance information	-	1	3
Lack of segregation of duties	-	-	-
Poor record keeping	-	-	4

3 LOOKING AHEAD

Assignment area	Timing per approved IA plan 2015/16	Status
Property Maintenance (7.15/16)	2013/14	Draft Report issued 7 October 2015
Project Management (9.15/16)	Quarter 4	Draft Report issued 22 October 2015
Contract Management (10.15/16)	Quarter 1	Draft report issued 23 October 2015
Income from recycling: green waste	Quarter 2	Deferred to December 2015 at management request
Income from car parking	Quarter 2	Fieldwork underway
Capital accounting and asset management	Quarter 3	
Facilities Management	Quarter 3	
Data Quality	Quarter 3	
Payroll	Quarter 3	
IT Audit	Quarter 3	
Performance Management and Delivery of Corporate Plan	Quarter 4	
Risk Management	Quarter 4	
Governance	Quarter 4	
Procurement	Quarter 4	
Fleet Management	Quarter 4	

4 OTHER MATTERS

4.1 Changes to the audit plan

There have been no changes to the audit plan to date.

4.2 Added value work

We have undertaken the following added value work since the previous Audit Committee.

Area of work	How this has added value
Our audit of project management and contract management were undertaken by a specialist in this area.	Our audit has provided the Council with a greater level of skill in these areas which has resulted in areas for management attention which may not otherwise have been determined. These reports are currently in draft for management review. .

4.3 Key performance indicators (KPIs)

Delivery				Quality			
	Target	Actual	Notes (ref)		Target	Actual	Notes (ref)
Audits commenced in line with original timescales	Yes	Yes	1	Conformance with PSIAS and IIA Standards	Yes	Yes	-
Draft reports issued within 10 days of debrief meeting	100%	75%	2	Response time for all general enquiries for assistance in 2 working days	100%	100%	-
Final report issued within 3 days of management response	100%	100%	-	Response for emergencies and potential fraud	1 working day	N/A 100%	-
Notes							
1 – Dates have been changed at the request of management							
2 – Reports were delayed earlier in the year. Delays now addressed.							

APPENDIX A: EXECUTIVE FINDINGS AND ACTION PLANS

Assignment: Attendance Management (1.15/16)	**Opinion:**	Green

The key findings from this review were as follows:

a) Attendance data is reviewed on an annual basis at Council level, the most recent data reported was from the end of the last financial year 2014/15. During 2014/15 there were reported to be a total of 2113.72 working days lost to staff absences. This represents an increase of 17% on the previous financial year 2013/14. This increase in the number of working days lost to sickness was put down to an increase in the number of days lost to long term absences. In contrast the number of working days lost to short term absence fell by 18% on the previous financial year.

b) The average number of working days lost per employee was 6.75, an increase on5.6 days in 2013/14 days, and which is above the Council's target of 6 days. From the Chartered Institute of Personnel and Development's national survey, the industry average for employee days lost to sickness is 8.2 days within the public sector. Despite the Council not meeting the target of 6 days per employee, it has performed well against the industry average as per the CIPD's benchmark figure.

Evidence of well-designed controls identified in our audit being effectively applied

c) The Council has in a place a robust set of policies and procedures with regards to the attendance management process at the organisation. The policy details how absences are to be dealt with and the strategies in place to mitigate sickness absence.

d) Policies and procedures should be accessible to all members of staff to ensure that all employees have a full understanding of the absence/attendance reporting procedure at the Council. The Councils absence policies and procedures are widely available to employees via the staff intranet.

e) Our substantive testing found that all dates input and recorded on iTrent were accurately supported by archived sickness certificates.

f) We confirmed that access to the iTrent system is restricted to appropriate users such as line managers and key HR personnel. Information stored on iTrent is password protected for use both by HR and the appropriate Line Manager. The cumulative monthly and quarterly reports are saved in the secure drive for HR use only. Line managers can produce mini reports for their sections which will illustrate trends and where triggers have been hit.

g) Each month the HR Information & Systems Officer ensures that the absence data on iTrent reconciles with employees self-certification documents and medical notes. For a sample of 10 we agreed these to the data on iTrent.

h) When individual absences hit a number of absences within a 12 month period, a trigger point is activated and a 'wellness review meeting' takes place between HR and the employee. The HR Team keep a record of individuals who have met the trigger point and their reasons for absence. For a sample of employees who had reached said trigger points we found that all had been subject to a 'wellness review meeting'. In addition all individuals sampled were present on a monthly 'trigger log'.

i) If an individual is off for a period of 8 days or greater they are required to provide a doctor's note to confirm that they were unfit to work. For a sample of employees who had been off eight days or longer a doctor's note was in place to explain the absence.

j) Where the Council is concerned for an employee's health or welfare or ability to carry out their role, it may ask individuals to attend a medical appointment with the occupational health provider. Within our sample of 10 long-term absences tested only three individuals were referred to occupational health, and where there is correspondence in place with the individuals GP it is often not deemed necessary. Where required, necessary documentation was in place to evidence that the occupational health meeting had taken place and the discussions carried out at the meeting.

k) If an individual is off for a period greater than two weeks medical notes should be in place to verify the reasons why the individual was off sick and cover the absence period. Where an employee has been absent for two months or more and there is no identified return date in the near future, the line manager will contact the employee to arrange an informal meeting to discuss the current situation and when a return to work can be reasonably expected. For a sample of individuals who were off long term sick none exceeded the two month point. For any absences greater than two weeks supporting consecutive medical notes were in place to explain the reason for the individual's sickness and to account for the length of the absence period.

We identified the following weaknesses where recommendations have been raised:

l) On an individual's return to work from a period of sickness absence a formal 'return to work' interview should take place between the employee and their line manager. For a sample of 10 individuals tested eight had not had a 'return to work' interview carried out. There is a risk that if back to work interviews are not being carried out on an employee's return any issues surrounding absences may not be fully addressed leading to further potential absences in the future.

m) On an individual's return to work they are required to complete a self-certificate form detailing the length of their absence and their reasons for not attending work. From a sample of ten individuals we found that two who had returned from work did not have a self-certificate in place detailing the length or reason for their absence. Without the information on the system being appropriately backed up with a self-certification form or medical note there is no way to confirm the length of an absence and the reasons as to why it has occurred. This creates the risk that absences are not appropriately recorded on the system and do not give a true reflection of the levels of absenteeism at the Council.

	Agreed Management Action	Implementation Date	Manager Responsible
1	On an employee's return to work an automated reminder email will be sent out to the employee and line manager to ensure back to work interviews are carried out and formally recorded on iTrent. In addition a member of the HR team will review ITrent on a monthly basis keeping a log of where back to work interviews are outstanding. Managers will be continually prompted by HR until the meeting has taken place and they can be removed from the log. (Medium)	July 2015	Shona Mason - Head of HR and Organisational Development
2	On an employee's return to work an automated reminder email will be sent to staff to ensure self-certificates are filled out and returned to Human Resources. Reminders will be continuously sent out until the form has been completed and returned to HR. (Low)	July 2015	Shona Mason - Head of HR and Organisational Development

Assignment: Recruitment (2.15/16)	Opinion:	Amber/Green

The key findings from this review are as follows:

We identified the following weaknesses:

a) There is a 4 year HR strategic resource plan in place which is due to be refreshed in April 2016. There is scope within this document for detailed analysis to assess future demand within the HR Team.
b) The Council does not formally review the effectiveness of advertising and recruitment methods for job posts at the organisation however alternative methods of advertising via different jobsites for example are considered if current methods are proving to be ineffective and costly.
c) Management annually report on the costs associated with recruitment each year. During 2014/15 there were a total of 52 recruitment campaigns. In addition the Council should look to incorporate non-financial measures when analysing recruitment. Such as:
   - Average number of applicants per job posting (volume)
   - Percentage of applicants who meet minimum job criteria (Quality)
   - Time taken to fill each job opening (effectiveness)
d) Agency staff details and checks are captured centrally by HR via monthly forms completed by Heads of Service and are recorded on a central spreadsheet. Managers locally currently have delegated authority to engage agency staff. These arrangements need to be reflected in the Council's HR policies and procedures.
e) Any new posts created at the Council must be authorised by the line manager and the appropriate director and evidenced via an REC01 form prior to the job being advertised. For a sample of 10 new roles at the Council we found that nine out of the 10 had been appropriately authorised as per the Council's policies and procedures. However for one position there was no REC01 form in place evidencing why the position had been created and who had authorised the advertisement of the job role. There is a risk that without proper authorisation and review, positions at the Council may be created where it may be inappropriate resulting in unnecessary staffing and recruitment costs.
f) As per the Council's policies and procedures all job advertisements at the Council should contain the following statement as part the organisations anti-discrimination policy 'We welcome applicants from all sections of the community.' We reviewed two current advertisements on the Council's website and found neither contained the anti-discrimination statement although the statement is detailed in full on the Council's Recruitment webpage. There is a potential risk that as a result of non-compliance that recruitment is not delivering against wider initiatives and anti-discrimination policies at the Council.

Evidence of well-designed controls identified in our audit being effectively applied

g) The Council has a policies and procedures for the recruitment process at the organisation. The policies cover full time employees, agency workers, part-time workers and individuals on fixed term contracts.
h) Policies and procedures regarding recruitment are widely available to staff at the organisation via the Council's intranet. In addition new managers are provided with training in relation to the recruitment policy when they first join the Council.
i) All applicants, internal and external, are required to complete an application form for any new post created; this is to ensure consistency in the application process and to comply with legislation on equality monitoring. For a sample of 10 individuals who took up posts at the Council an application form was on file for all.
j) Role profiles advertised by the Council set out the key responsibilities, accountabilities and the scope of the job. Furthermore the profile set out the minimum experience, skills, knowledge and abilities necessary to do the job satisfactorily.

k) All individuals present during a candidate's interview should have received formal training on the processes involved with vetting a candidate. For a sample of five managers at the Council who were present at candidate interviews, we found all had received formal training on November 2013.
l) Depending on the seniority of position advertised at the Council certain criteria has to be met with regards to the constitution of the interview panel.
m) For a sample of 10 individuals interviewed at the Council we found that the appropriate numbers of individuals were on the interview panel. The individuals on the panel were appropriate for the level of position being interviewed for.
n) The Human Resources Team annually produce statistics with regards to anti–discrimination and diversity monitoring at the Council. We were provided with the latest report from the end of the last financial year

2014/15. The report detailed various statistics such as gender, sexuality, and ethnicity of candidates who applied for roles at the Council.

o) Prior to employment at the Council individuals are subject to various pre-employment checks to ensure the candidates selected are appropriate for the roles they've applied to. For a sample of 10 new employees we found that all had two references on file and in addition where required, evidence of their academic achievements was on file.

p) We satisfactorily verified that pre-employment checks had been undertaken for a sample of agency workers engaged by the Councils Depot and that the central HR team had been notified of these details.

	Agreed Management Action	Implementation Date	Manager Responsible
1	The HR strategic resource plan for 2016 -2020 will include detailed analysis of employment trends, turnover rates and expected resource demands for the HR section. (Low)	April 2016	Head of HR & OD
2	There will be improved compliance to ensure all REC01 forms have been completed and are on file, and these will be routinely checked. (Low)	1st Jul 2015	Head of HR & OD
3	The Council's policies and procedures will be updated to reflect the fact the depot has delegated authority to carry out background checks and store employee data for all agency staff. (Low)	1st Oct 2015	Head of HR & OD
4	The Council agreed to ensure that all anti-discrimination statements as detailed in the 'recruitment selection toolkit' will be included in all job advertisements to ensure the council is effectively delivering against wider initiatives with regards to diversity and discrimination. The job advertisement checklist currently used will be amended to include a check that such statements are present. (Low)	22nd June 2015	Head of HR & OD
5	A regular review whether the current methods for advertising are effective will be undertaken along with the use of alternative methods of advertising via other jobsites if current methods are proving to be ineffective and costly. Measures of effectiveness could include - Average number of applicants per job posting (volume) - Percentage of applicants who meet minimum job criteria (Quality) - Time taken to fill each job opening (effectiveness) The use of and cost effectiveness of the employment agencies used by the depot will be reviewed. (Medium)	1 July 2015	Head of HR & OD

6	Management will look at incorporating non-financial indicators into performance monitoring. Indicators could include the following: - average time to fill a position from point of advertising; and - Turnover rate (how often positions are re-advertised). (Low)	1 April 2015	Head of HR & OD

Assignment: Review of Anti-Fraud and Anti-Bribery Arrangements 3.15/16	Opinion:	Advisory

a) In assessing the Council's resilience to fraud and bribery we were unable to identify any specific risk that exposed the Council to attack either internally or externally. However, we identified that the Council's strategic approach around raising awareness to fraud and bribery is lacking, and these underpin the culture and awareness of the organisations response to fraud. Our overarching recommendation is that the Council streamlines its strategic approach to encompass anti-fraud and anti-bribery awareness training that should be supplemented with:
- Leaflets, flyers and anti-fraud and bribery literature,
- A dedicated internal and external web-page
- Clearly defined whistleblowing procedures or other reporting mechanisms.

b) The Council must recognise that its main defence against fraud and bribery is its staff. Control measures alone will not stop or prevent fraud or bribery. The focus must be on prevention rather than cure. It is far easier and more cost-effective to prevent fraud and bribery than it is to investigate them and seek redress. One of the most effective means of preventing fraud and bribery is to increase the perception of early detection and a robust response. This message must be endorsed by a strong statement that promulgates swift and certain action where instances of fraud and bribery are identified. The simplest and most cost-effective way of achieving this is through a programme of education where staff are educated as to the risks, how to recognise the warning signs, and how to report concerns. However, for this to be effective, staff must have confidence that their concerns will be taken seriously and that they will not face reprisals for raising legitimate concerns. This message must be endorsed with a consistent tone from the top which commits to a zero tolerance approach.

	Agreed Management Action	Management Comment	Manager Responsible
1	The Council should streamline its strategic approach to include anti-fraud and anti-bribery awareness training that should be delivered as part of an induction process. Having been delivered at induction the training should include a continuing rolling process of bespoke fraud and bribery awareness sessions delivered on a yearly or bi-yearly basis. These session should be supplemented with: • Leaflets, flyers and anti-fraud and bribery literature • A dedicated internal and external web-page A clearly defined whistleblowing or reporting mechanism. (High)	This will be incorporated into the Corporate Governance Action Plan and training will be developed. Initial training will be given to the Leadership Team and bi yearly awareness sessions will be established The induction training will be reviewed to ensure it adequately reflects the Council's approach to fraud.	G McTaggart S Mason (induction training) Dec 2015

2	The Council should conduct an on-line assessment / questionnaire to measure the level of anti-fraud and anti-bribery awareness within the Council. The results of the assessment should form the basis of an educational awareness package for both new starters and existing employees. This could include an online training module, training workshops, development of a counter fraud webpages and the distribution of anti-fraud and anti-bribery publicity material. (Medium)	As part of awareness campaign, we will introduce posters and signposts. There will be dedicated information on both the web site and intranet and an online assessment is not considered beneficial as awareness sessions will be bi yearly.	
3	It is recommended that the Council reviews documentation and forms where a declaration is made to the effect that the information provided is true and accurate. Examples of such forms would include: • Job applications forms • Expense claim forms • Housing application forms • Council tax application / change of circumstances forms. An example of a more robust declaration is highlighted below: I declare that the information I provide on this application is true and accurate. I understand that if I have provided any false, misleading or inaccurate information, then my application may be rejected or that I may be subject to disciplinary proceedings which could amount to my dismissal and or action being taken against me in the civil and criminal courts for offences identified under the Fraud Act 2006 / Housing Act… (Medium)	As documentation is reviewed we will enhance the declaration within the forms to strengthen the declaration. A review will be undertaken by the Corporate Governance Group to look at the documents to be updated.	April 2016 Corporate Governance Group

4	The Council should ensure that the following polices dovetail with one another and there is a clear signpost that links to the other policies and that throughout all policies a firm tone from the top endorses a zero tolerance approach to instances of fraud and bribery: • Anti-fraud, Anti-bribery Strategy and Whistleblowing Policy • Fraud Response Plan • Anti-bribery Policy • Codes and protocols • Procurement tool kit • Financial regulations • Anti-money Laundering Policy. This would ensure a more streamlined and consistent approach to the Council's strategic objectives of creating an anti-fraud culture. (Medium)	These policies will be reviewed and updated in line with best practice to ensure they are more streamlined. The relevant Heads of Service will be responsible for updating their documents.	G McTaggart & Relevant Heads of Service April 2016
5	The Council should ensure that the following policies place a clear expectation upon all staff to conduct their affairs in such a manner as not to expose the Council to the risk of fraud or bribery and that all suspected instances of fraud, bribery and bribery are reported at the earliest opportunity: Anti-fraud, Anti-bribery Strategy and Whistleblowing Policy Fraud Response Plan Anti-bribery Policy Codes and protocols Procurement tool kit Financial regulations Anti-money Laundering Policy Ethics Policy Discipline Policy Employment contracts Procurement policy. (Low)	This will be reviewed by the Corporate Governance Group and form part of their Action Plan	G McTaggart December 2015
6	It is recommended that the Council make a clear expectation of all staff and members to report instances of suspected fraud and bribery without delay. This expectation needs to be communicated in the following policy documents and literature: Anti-Fraud and Bribery Policy Ethics Policy Discipline Policy Whistleblowing Policy Financial Regulations Employment Contracts Procurement Policy. (Medium)	Council Officers are expected to report all suspected fraud or bribery. As part of the awareness sessions this message will be strengthened and the policies will be reviewed and updated as necessary.	Corporate Governance Group December 2015

7	The Council should review its use of agency staff and insist that agency providers provide written confirmation of the post holders suitability to fulfil the role within the Council and that the agency has conducted background checks to ensure the post holders suitability to fulfil the role within the Council. (Medium)	The Council have received a separate report on Agency Procurement identifying a number of issues. These are currently being addressed and a report went to Strategy & Resources Committee 24th June 2015 to agree the way forward. This will reduce reliance on agency staff as well as ensuring adequate checks are undertaken by the agreed Provider.	December 2015
8	Once anti-fraud and anti-bribery awareness training sessions have been delivered, the Council should introduce a system / mechanism for recording all referrals made. This would allow the Council to conduct a root cause analysis of any suspected or identified misbehaviour and this should be used to inform future fraud and bribery disruption strategies. (Low)	All instances of fraud will be raised through the Corporate Governance Group to review the cause, highlight any weaknesses in controls and the action required to strengthen controls	Gillian McTaggart immediately
9	In producing the ICT Acceptable Use Policy, the Council should include a specific reference and paragraph to the implementation of a lawful business monitoring protocol. This enforces the legal position of the Council to monitor and review IT and telephone systems for the prevention and detection of crime. (Low)	A separate lawful business monitoring protocol is not required but the Head of ICT will ensure wording is strengthened	Mark Lumley December 2015

Assignment: Cash Handling (4.15/16)	Opinion:	Amber/green

The key findings from this review are as follows:

a) There are currently no corporate cash handling procedures. These are particularly required to prescribe standards and define those controls expected across the organisation. There is particular merit in issuing such instructions at the time of the closure of the cash office to ensure local officers are aware of their responsibilities in accounting for such transactions.

b) As part of this review we particularly sought to examine a number of areas where cash handling risk was considered to be high. These were areas where volumes of transactions were low but values high (deceased estates), where customers have been resistant to the use of other methods of payment or where cash continues to be received at sites other than cashiers (Gypsy Site Rents / Market Traders). From our testing of 20 historic transactions, interviews with responsible managers and direct observation of cash receipting and reconciliation processes we are assured that there is generally sufficient control in cash handling, security and documentation with adequate separation of duties. Our work did highlight a number of significant exceptions. In particular from our detailed testing we found:

c) Gypsy site rents receipts were not being issued by the rent officer for monies collected and in this respect any allegations of fraud or irregularity could not be systematically refuted. Additionally at the time of our audit we were informed that the rent accounting system had not been operating for more than 6 months due to software problems and that individual rent accounts were not active. Rent payments at the time of the audit were being posted to a holding account pending system correction.

d) The Officer collecting Gypsy rents is taking the cash home with him after Friday collections and bringing it back to the Town Hall for deposit with Cashiers on a Monday. (Cash levels range between £50 and £200).

The transport of such cash sums provides for an increased risk profile.

e) A large cemetery cash payment was received (£4K) in respect of funeral arrangements in March 2015. This payment was received in person by the Cemetery Officer from bereaved relatives after the Cash Office had closed and was in respect of a funeral the following day. It was held securely overnight at the Town Hall before being passed to the Cash Office the following day. After the closure of the Cash office in November there is potential for increased risk in such areas as cash payments will continue to be tendered directly by the public.

f) Procedures in place for deceased estates are clear and satisfactory and our sampling confirmed that cash counted and taken from site is evidenced by the signature of two officers. Sums of cash involved can on occasion be large and in excess of £1k although on average only 2 cases a year occur.

g) A small minority of Market Traders refuse to set up direct debit payment processes via the debtors system and continue with cash payments. Receipting and documentation of these transactions is satisfactory although resource intensive and costly to administer.

h) Our sampling satisfactorily verified adequate detail regarding cash transactions selected and posted via the cash receipting system and banking processes. The Exchequer Service Team reconciles Cash Office receipting systems and those external bankings made by other service depts. These reconciliations are tested as part of our annual key audit programme and were last reported in our finalised report dated March 2015.

i) We satisfactorily carried out direct observation and walkthrough testing of cash transactions that came through the Post opening and drop box processes at the Town Hall and that handed into the foyer receptionists.

j) We verified that a business case and rationale has been agreed by the management team regarding the closure of the public cashier service and is to be offset by the promotion of alternative methods of payment such as:
- A night safe facility so that deposits can be made when the Cash Office facility is closed. This will enable payments still to be taken at the Town Hall, but it would be made clear that no receipt will be given for these payments;
- A telephone with restricted access to be sited by the Cash Office that will allow customers to make payment by credit or debit card;
- The use of kiosks placed in the Civic Street where customer can make payment using the web;
- Other methods of payment that will also be promoted such as paying through their bank and using the Council's website.

k) At the time of our audit a project plan had not been created to monitor and report upon progress of the cash office closure. Management have agreed that a project plan must be drawn up to provide a clear timeline of those actions and responsibilities that will be required to implement this objective. In particular we would recommend (and management have agreed) that a project risk register is also created to accompany the detailed project plan. This would list specific risks and actions and particularly those service areas which will be significantly impacted by the closure. Those discussions and alternative arrangements for cash collection which are currently underway should be documented here and any residual risk highlighted for consideration of the management team. A monthly update to the register will be reported to the management team in the period leading up to the actual closure.

l) From our research of other Authorities (see 3.3.2) we note that Epsom continues to accept and offer cash transactions at levels significantly higher than neighbouring Councils. In the longer term a strategy is required to reduce further the reliance on cash transactions through Council Offices. One neighbouring Authority (Reigate and Banstead Borough Council) has taken the view that cash transactions will not be accepted at any Council site and this is not offered as an option to Customers. Cash can only be accepted as a payment to this Council by way of a transaction at a UK bank. This decision was arrived at after demographic and consultancy research within the Borough demonstrated that the public were now very comfortable with electronic payment methods and online transactions. In this respect they sought to align Council income systems with this cultural shift whilst also improving and updating their CRM processes and realising significant overhead savings. Other neighbouring Authorities are on a similar journey to minimise cash transactions with a future view to similarly withdrawing these type of transaction altogether.

	Agreed Management Action	Management Comment	Manager Responsible
1	Corporate cash handling procedures will be produced to prescribe standards and define those controls expected across the organisation. Management agree that there is particular merit in issuing such instructions at the time of the closure of the cash office to ensure local officers are aware of their responsibilities in accounting for such transactions. (Low)	November 2015	Head of Financial Services
2	Local procedures must make clear: - who is responsible for collecting and receipting cash transactions - the audit trail and local documentation for recording such transactions - the secure retention and banking of cash - processes for ensuring cash collected is reconciled to postings in the accounting ledger. Where appropriate these procedures will also need to be updated to take account of the closure of the Cash Office. (Low)	December 2015	Services Managers / Head of Financial Services
3	Signed receipts will be issued for all gypsy site rent transactions. A copy of this will be retained and the receipt number recorded on the weekly collection sheets held. Once operational again up to date rent accounts will be posted with historic rent debit and payment transactions for 14/15. (High)	November 2015	Gypsy Liaison Officer
4	Gypsy rent collection –Management agree that the taking of cash home must be avoided if at all possible. Other options such as banking the cash on Friday at a local bank rather than waiting for the Cash Office will be explored or collecting the rents at a different time / day. (Medium)	November 2015	Gypsy Liaison Officer

5	A project plan will be drawn up to provide a clear timeline of those actions and responsibilities that will be required to progress the closure of the cash office. In particular management have agreed that a project risk register is also created to accompany the detailed project plan. This will list specific risks and actions and particularly those service areas which will be significantly impacted by the closure. Those discussions and alternative arrangements for cash collection which are currently underway will be documented here and any residual risk highlighted for consideration of the management team. A monthly update to the register will be reported to the management team in the period leading up to the actual closure. (Medium)	October 2015	Head of Financial Services
6	In the longer term the Exchequer Team Leader agrees that a strategy is required to reduce further the reliance on cash transactions through Council Offices. This consideration will be further developed in in action plans intended to encourage electronic payments and only accept cash via banking. (Medium)	April 2016	Head of IT / Financial Services

Assignment: Venues (5.15/16)	Opinion:	Amber/green

There is an appropriate control framework established.

We identified that the Council does not have a strategic plan with regards to the operations of its venues. There is a risk that without a strategic plan any opportunities for cost saving, marketing and income improvement opportunities may not be identified and as a result are unlikely to be realised by the Council over the coming years.

Application and compliance with the Control framework:

We confirmed that the controls are generally complied with in practice with one exception.

Annually the Council reviews and update the schedule of rates charged for the hire of venues to the general public. These are then updated on IRIS and on the Council's website. For the Longmead Social Centre the schedule of rates had not been updated and was still being advertised as the rates agreed in the last financial year on the Council's website. There is a risk that customers having agreed to pay the rate as per the Council website may be unwilling to pay the rate agreed by the Council.

We identified the following areas where the Council had well-designed controls in place:

a) Venue fees and charges are reviewed annually as part of the Council's budget setting process. These are then ratified by the Council prior to the start of each financial year. This year's annual uplift in fee parameters was ratified by the Council on 17 February 2015.

b) Once fee parameters have been agreed for the new financial year they are updated on IRIS. For a sample of payments made we found the amount charged as per the invoices reconciled to the newly agreed schedules of rates agreed by the Council.

c) Once the venue has been booked for hire a debtor invoice is raised for the amount due and for payment prior to the event. For a sample of payments we found that the value on the invoices matched those on

the accounting ledger and the receipts of income matched to debtor invoices.

d) Any expenditure against the budget for venue management is carried out in line with the Council's policies and procedures. Once a purchase order has been raised it must be approved by an authorised office. For a sample of 10 invoices paid we found that all payments had been appropriately approved and segregation of duty was present.

e) Monthly aged debtors reports are produced by the Finance Team, and where necessary outstanding debts are identified and chased up by Finance Administrator.

f) Debt recovery at the Council is undertaken through using a combination of reminder and direct contact with the debtor to pursue arrears and all recovery action is recorded on the notes facility within ledger. Where a debt cannot be recovered it is passed onto legal. We confirmed that for our sample of invoices sufficient attempts were made to recover the Council's debts.

g) Managers are provided with monthly budget monitoring reports detailing expenditure at the Venues against budget; these are reported from the ledger. *It is up to individual managers and accountants to decide how regularly they should meet, but as a minimum they meet quarterly.*

h) Tendering of services for all venues operations is in line with those as per the Council's procurement policies and procedures. The Council has not procured for any services in relation to venues management since 2006. The last two procurement activities carried out were for catering contracts worth a combined total of £40k.. We are aware that the Council is focussing on procurement activities as a separate exercise and so we have not looked in to this or raised any management actions.

	Agreed Management Action	Management Comment	Manager Responsible
1	The Council has a timetable for the completion of a venues marketing and cost saving plan. The plan will address: - how the Council aim to increase revenue; - how the Council aim to cut costs; - a marketing plan; and - future forecasted spend on improving the venues. (Medium)	31 March 2016	Andrew Lunt - Head of Venues and Facilities
2	The Council will amend the website to reflect new price plan the Council has in place for the Longmead Social Centre. (Low)	30 September 2015	Andrew Lunt - Head of Venues and Facilities

Assignment: Information Governance (6.15/16)	Opinion:	Amber/green

a) The Data Protection Policy and IT Security and Acceptable Use Policy are communicated to staff with additional guidance notes. Both policies are clear and detailed and seek to ensure that the authority maintains and uses data that is fully compliant with legislative requirements and meets the business and information needs of the Council. The Data protection Policy recognises that the Council is acting as custodians of personal data which can often be of a sensitive nature. It acknowledges its legal and moral duty to ensure that data is handled properly and confidentially at all times, irrespective of whether held on paper or by electronic means. The Security Policy particularly seeks to prescribe controls in respect of:

- System Integrity
- Physical / Software Security
- Passwords
- Laptops / Portable Devices
- Approved Email use (Internal and External)
- Remote Use of network
- Approved Use of Internet
- Telephone System Use

i) Staff are required to sign a declaration of receipt and understanding of these policies. These declarations are held on staff HR files. From our testing of 5 staff (including one casual) we found that HR held a declaration for 4 staff in respect of the IT Security Policy and from 2 staff in respect of the Data protection Policy.
Going forward a further sweep and refresh of this process is required to ensure all staff are covered by such declarations. (We note that in order to improve the consistency and record of training and Policy Acceptance, a number of Councils are now using e-policy software and in this respect EEBC should consider the organisational efficiency benefits of such applications)

j) Similarly Councillors are required to sign a declaration of receipt and understanding of these policies and we found evidence that this is evidenced for newly appointed members. We could not verify a declaration for one of our sample who was a Councillor with longer service and in this respect further assurances are required to ensure all members are covered.

k) Clear procedures and controls have been prescribed in respect of data retention and these are available online through the LGA website and are referred to in the EEBC Information Assurance Policy. The guidance is categorised by the types of records that could be kept for each service to ensure compliance with Section 12 of the Lord Chancellor's Code of Practice on the management of records and to meet likely business needs. The guidance is put together by Kent County Council's Legal Services team (for the LGA). It describes how long records need to be kept before destruction or transfer to the archives. This guidance is routinely updated but can only be accessed through a secure login to the LGA website which is held by the Head of Legal Services. There is potential scope for a more accessible and easier reference document to be produced and made available to EEBC staff.

l) There is not currently an Information Asset Register and this absence weakens overall assurances that all data is identified controlled and securely maintained. Such a register would provide a single point of reference for recording all known data sets within the organisation. It would help to identify risk, duplication and an aid in ensuring compliance with regulatory obligations as well as good housekeeping when data, staff or services migrate.

m) Each individual is responsible for the security of any Laptop/portable device they use and policy requires that no sensitive or personal information relating to individuals is to be held on the hard disk of a portable device. Furthermore EEBC data is secured in a Citrix virtualised environment and is only held on central servers.

n) Routine IT back up cycles are in existence and recovery testing of back up media with the external continuity provider is normally undertaken on an annual basis. This provides assurance that data held can be successfully restored. We understand that this testing has not taken place however in the last 12 months and a management action has been agreed to progress this. In addition a management action has

been agreed to produce an ICT Disaster recovery plan which will provide a structured approach for responding to unplanned incidents that threaten the IT infrastructure and business continuity.

o) Our testing would indicate that relationships with all key partners satisfactorily consider information governance. In particular The Surrey Multi-Agency Information Sharing Protocol (MAISP) is an agreed set of principles about sharing personal or confidential information. This enables each organisation signed up to the protocol to understand the circumstances in which it should share information and what its responsibilities are. This protocol is agreed with key partners such as the Police, NHS, County Social Services, Community Groups and neighbouring Local Authorities. In order to communicate the requirements in the MAISP, a management action will ensure that reference to the Data Sharing Protocol will be included in the ICT Acceptable Use Policy with particular reference to the controls and checklist documents prescribed

p) This audit has also highlighted the absence of Information Governance incident log which would consistently record incidents, outcomes and how controls are improved going forward. As a result of early discussions in progressing our work a log was being created to coincide with the completion of this audit.

	Agreed Management Action	Management Comment	Manager Responsible
1	An Information Asset Register will be produced and maintained. This will provide a single point of reference for recording all known data sets within the organisation. It will help to identify risk, duplication and be an aid in ensuring compliance with regulatory obligations as well as good house-keeping when data, staff or services migrate.	1April 2016	Simon Young
2	Going forward a further sweep and refresh of HR files will be undertaken to ensure all staff are covered by ICT security and data protection declarations.	1April 2016	Simon Young
3	Going forward a further sweep and refresh of all Councillor records will be undertaken to ensure all Members are covered by ICT security and data protection declarations.	1April 2016	Simon Young
4	Access to the LGA document retention guidance will be made more easily accessible for all EEBC staff and/or reproduced in a format that can be more immediately referred to. On an annual basis the Data Protection Officer will send a reminder to all responsible officers to archive or destroy information in accordance with this guidance.	1April 2016	Simon Young
5	An Information Governance Incident Log will be maintained. Such a log will consistently record incidents, outcomes and how controls are improved going forward.	30 September 2015	Simon Young
6	The Data Protection Officer will formally request feedback from the Head of IT on an annual basis that security breaches have been recorded and investigated where appropriate and that system integrity has been maintained.	1 April 2016	Simon Young / M Lumley
7	All business critical systems will be tested and restored with the external provider on at least an annual basis.	1 April 2016	M Lumley
8	An ICT disaster recovery plan will be produced that will provides a structured approach for responding to unplanned incidents that threaten the IT infrastructure and business continuity. It will include hardware, software, networks, processes and people	1 April 2016	M Lumley
9	Reference to the data sharing protocol will be included in the ICT Acceptable Use Policy with particular reference to the controls and checklist documents prescribed.	1 April 2016	Simon Young

Assignment: PCI Compliance Control Framework (8.15/16)	Opinion:	Amber/red

Given the nature of the review and current Council PCI non-compliant status, the methodology focus was based on controls design.We identified a number of weaknesses in the design of the control framework that impact on PCI compliance, principally:

a) The Council has no clear view of who is responsible for the identified PCI actions to be implemented to ensure PCI compliance. There is a need for more formal roles and responsibilities.

b) The Council records inbound voice calls to assist with staff training and provide performance management and issue resolution. The calls are recorded using the VPI call recording system. We noted during the review of VPI the recording solution is not PCI compliant. This prohibits PCI accreditation.

c) No specific PCI training programme is in place. In addition, whilst the Council's security policy covers the Data Protection Act (1998), the policy does not highlight the importance of PCI information for users that process PCI data.

d) There is a current absence of a complete process to review and verified the PCI certification of the 3rd party vendors.

However, we did note the following:

e) The Council was quick to respond and amend the Action Plan with the new findings.

f) Although no formal PCI training was in place, there was no breach in handling of PCI data as a result of the informal training that was given.

g) The Action List the Council has drafted shows great effort in the remediation and understanding of PCI.

	Agreed Management Action	Management Comment	Manager Responsible
1	The Council will formalise training, policy and procedure and train and communicate them to the relevant staff and take a risk based approach to training staff who handle PCI data and formally have a training program implemented. (Medium)	30 September 2016	Lee Duffy, Head of Financial Services
2	Draft a Policy that relates specifically to PCI and communicate it to the required personnel. (Medium)	30 September 2016	Lee Duffy, Head of Financial Services
3	Draft a Scope and Policy Mapping Matrix that shows the PCI environment as well as the scope of the PCI environment. (Medium)	30 September 2016	Lee Duffy, Head of Financial Services
4	The Council should draft a PCI Data Flow Diagram. (Medium)	30 September 2016	Mark Lumley, Head of ICT
5	The Council will draft a 3rd party PCI compliance tracking sheet and track their PCI status annually. (Medium)	30 September 2016	Lee Duffy, Head of Financial Services
6	The Council has now enquired with Adelante to their current PCI status and take action accordingly and has received assurance from Adelante that they are PCI Compliant. (Medium)	11th November 2015	Mark Lumley, Head of ICT
7	The Council will ensure that the chosen call recording software that 'records' conversations in scope of PCI is PCI compliant. (High)	31 Match 2016	Mark Lumley, Head of ICT

8	The Council will ensure that only authorised people have access to view the PCI data that is entered on the screen. The Council could add a privacy filter to the screen to block out the cameras view of the screen once the information on which screen has been provided by RSM. (High)	30 September 2016	Lee Duffy, Head of Financial Services
9	Identify roles and responsibilities that govern the PCI environment and communicate the responsibilities to everyone. (High)	31 March 2016	Kathryn Beldon, Director of Finance and Resources.

FOR FURTHER INFORMATION CONTACT

Karen Williams

karen.williams@rsmuk.com

Tel: 07818 002463

rsmuk.com