Appendix B

FINAL AUDIT REPORTS ISSUED SINCE LAST MEETING

	Audit Title	Date Issued	Opinion Framework/Control
1	IT Security 2013/14	20.6.14	Good/Satisfactory
2	Planning & Development Control 2013/14	1.8.14	Satisfactory/Satisfactory
3	Cash & Bank Reconciliations 2013/14	1.8.14	Good/Good
4	Main Accounting 2013/14	1.8.14	Good/Good

Appendix B

Review of IT Security 2013/14 **Issued 20 June 2014**

Opinion: Control Framework – Good (Previous year - Satisfactory)
Compliance with Framework – Satisfactory (Previous year - Unsatisfactory)

The purpose of the review was to provide an assurance regarding the effectiveness of the arrangements in place for IT Governance and Security, as well as the effectiveness of service delivery and fitness for purpose.

To this effect, the following key risks and controls were examined:

1) Risk that the Council may not have a well-defined IT Governance framework in place, leading to ineffective management control and non-compliance with statutory obligations.
2) Risk that the Council may not have adequate control over data security leading to unauthorised access.
3) Risk that lack of implementation of recommendations leading to non-compliance with pertinent legislation.
4) Risk that IT arrangements may hamper the efficient delivery of shared services.
5) Risk that IT Assets may not be adequately protected leading to misappropriation and fraud.
6) Risk that IT risks may not be fully considered and evaluated resulting in unauthorised access, error and fraud.

Audit testing results indicated that controls were fully met in two of the aspects examined, whilst four aspects were partially met in relation to compliance (Risks 2, 3, 4 and 6).

The opinion of the auditor was that the framework of controls for the IT Security system was “good”. Compliance with the framework was found to be “satisfactory”. This meant that a high level of control framework was in place to ensure the achievement of service objectives, good corporate governance and to protect the Council against foreseeable risks. There was evidence that occasional instances of failure to comply with the control process were identified and opportunities still exist to mitigate further against potential risks.

The following four recommendations were agreed with Management to address the areas where controls were partially met. These relate to risks 2, 3, 4 and 6.

- Consideration needs to be given as to how access controls can be monitored for temporary/contract staff. Also consideration needs to be given to current physical access controls and whether access to certain areas should be fully restricted to IT only. An external review of environmental controls must be undertaken.

- The IT Service Manager needs to ensure that the Disaster Recovery plan is completed with links to the Corporate Plan.

- In terms of ensuring responsibilities and reporting lines are clear to both IT staff and customers, Operation Level Agreements (OLAs) should be drawn up between the SDC and DBC IT Teams with Service Level Agreements (SLAs) between both IT Services and relevant customers.

- The IT Service Manager reviews existing arrangements and ensure that they are effective to reduce IT related risks. This would include

    - Examination of the current Strategic Risk Register and Operational Risk Register and identifying any gaps.

    - Examination of internet access over the public wireless network

.

Members will be advised of the progress in implementing these recommendations in due course.

Review of Planning & Development Control 2013/14 **Issued 1 August 2014**

Opinion: Control Framework – Satisfactory (Previous audit - Satisfactory)
Compliance with Framework – Satisfactory (Previous audit - Satisfactory)

The purpose of the review was to provide an assurance regarding the effectiveness of the arrangements in place for the management of the Planning & Development Control operations in meeting its service objectives. There have been some substantial changes within the team in recent months since the previous review in 2010/11.

To this effect, the following key risks and controls were examined:

1) Risk that the Council may not comply with relevant legislation, policy or good practice.
2) Risk that legislation and regulation changes may not be addressed or complied with.
3) Risk that the validation process may not be sufficiently robust or consistently applied.
4) Risk that planning enforcement may not be appropriate, expedient or consistently applied.
5) Risk that planning decisions could be overturned after an appeal and costs may be incurred.
6) Risk that timetables, deadlines and milestones may not be met.
7) Risk that the scheme of delegation and delegated powers may not be correctly applied.
8) Risk of fraud and/or corruption.
9) Risk that opportunities to demonstrate efficiency or VFM may not be maximised.
10) Risk assessments may not be adequately undertaken and risks not adequately managed.

Audit testing results indicated that controls were fully met in four of the aspects examined, whilst six aspects were partially met in relation to compliance. (Risks 3, 4, 5, 6, 7 and 8). However, the impact of non-compliance was relatively minor and in the main, there were compensating controls in place.

The opinion of the auditor was that the framework of controls for the Planning and Development system was "satisfactory". Additionally, compliance with the framework was also found to be "satisfactory". This meant that controls exist to enable the achievement of service objectives, obtain good corporate governance and mitigate against significant foreseeable risks. Occasional instances of failure to comply with the control process were identified and opportunities still exist to mitigate further against potential risks.

Nineteen recommendations were agreed with Management to address the areas where controls were partially met. These relate to risks 3,4,5,6 and 7. Most of the recommendations have already been implemented following management feedback. The outstanding key recommendations are set out below:

- Introduce procedures to review and update public Council website pages. A quick and easy way to highlight website pages that could be out of date or in need of review would be to ask IT to produce a webpage hit rate report. The pages with the lowest number of views could then be reviewed periodically to ensure they were still current and up to date as the low hit rate might be indicative of the page being out of date or needing to be deleted.

- Case Officers must sign and date the Green Validation Checklist prior to processing a case to evidence they agree the fees are correct and validation checks undertaken by the Validation Officer are complete and correct.

- Officers' delegation letters should include financial limits and clear referral instructions to obtain higher levels of approval if these financial limits are exceeded related to their delegated responsibilities. This should also include the Chief Planning Officer where very large cases are involved even though these cases would likely go to other senior officers, Development Control Committee and likely involve Council/Cabinet.

- Relevant findings and recommendations within this report should be addressed and built into the departmental Procedures Manual review currently being redrafted together with other associated departmental documentation to ensure controls and procedures are improved and risks mitigated
  .

Members will be advised of the progress in implementing these recommendations in due course.

Appendix B

Review of Cash & Bank Reconciliations 2013/14 **Issued 1 August 2014**

Opinion: Control Framework – Good (Previous year - Good)
Compliance with Framework – Good (Previous year - Good)

The purpose of the review was to provide an assurance regarding the effectiveness of the reconciliation process, which ensures the accuracy of the Council's accounting records as required by statute. Key areas examined, in addition to the reconciliation process, were timeliness and the promptness of actions taken to address unexplained variances.

To this effect, the following key risks and controls were examined:

1) Risk that the Council may not comply with relevant legislation, policy or good practice.
2) Risk that appropriate records are not kept to support the reconciliation process.
3) Risk that reconciliations between the Council's bank statement and financial systems may not be accurate, independent, up-to date or reviewed by a senior officer.
4) Risk that reconciliations may not be completed on a timely basis.
5) Risk that the Council may not have an accurate view of its cash flow or financial position.
6) Risk of fraud and/or corruption.
7) Risk that opportunities to demonstrate efficiency or VFM may not be maximised.
8) Risk assessments may not be adequately undertaken and risks not adequately managed.

Audit testing results indicated that controls were fully met in all of the aspects examined. One aspect of control was identified in relation to risk 3 where further enhancement would be beneficial. This is set out below.

The opinion of the auditor was that the framework of controls for the cash and bank reconciliation system was "good". Additionally, compliance with the framework was also found to be "good". This meant that a high level of control framework was in place to ensure the achievement of service objectives, good corporate governance and to protect the Council against foreseeable risks. There was evidence that the framework of controls were substantially being complied with and the risk management process was considered to be good. Only minor errors or omissions were identified.

The following recommendations were agreed with Management to address the areas where controls enhancements could be made. This relates to risk 3.

Agresso:

I. The number of 'super users' should be reviewed and reduced to a more appropriate level subject to the departmental operational needs.

II. Internal IT and external remote 'super user' profiles to be deactivated and only reactivated for the short duration of specific projects

III. Tandridge District Council 'super users' profiles to be restricted to Tandridge data only to prevent unauthorised access to Sevenoaks data.

IV. Activity reports to be produced regularly for all 'super user' profiles to monitor unusual or unexpected activity such as profile access set up, password changes, profile changes, system activity outside of expected 'day to day' role responsibilities to mitigate and reduce the risks of unauthorised activity.

TASK:

Bearing the above in mind for TASK there needs to be additional 'Super user' access in the event that the Finance and Admin Manager – Direct Services leaves at short notice, or is incapacitated for any length of time at short notice which would compromise day to day operations or activities. The IT team should be given a formal 'super user' profile so they can access the system and to monitor audit trails. We would also recommend that activity reports are produced and reviewed regularly as per IV) above.

Members will be advised of the progress in implementing these recommendations in due course.

Review of Main Accounting 2013/14 **Issued 1 August 2014**

Opinion: Control Framework – Good (Previous year - Good)
Compliance with Framework – Good (Previous year - Good)

The purpose of the review was to provide an assurance regarding the effectiveness of the controls over entries to the main accounting system. Key areas examined were the completion of data processing; accuracy and authentication of data.

To this effect, the following key risks and controls were examined:

1) Risk that the Council may not comply with relevant legislation, policy or good practice.
2) Risk that relevant records of transactions may not be current, accurate or complete.
3) Risk that transactions may not be allocated to their correct cost centres or accounts.
4) Risk that miscodings or variations may not be identified or appropriately reported.
5) Risk that financial data may not be presented in a way that is clear for non-financial managers to understand.
6) Risk of fraud and/or corruption.
7) Risk that opportunities to demonstrate efficiency or VFM may not be maximised.

8) Risk assessments may not be adequately undertaken and risks not adequately managed.

Audit testing results indicated that controls were fully met in all of the aspects examined. One control that came under risk 8 has been highlighted where enhancements can be made.

The opinion of the auditor was that the framework of controls for the main accounting system was "good". Additionally, compliance with the framework was also found to be "good". This meant that a high level of control framework was in place to ensure the achievement of service objectives, good corporate governance and to protect the Council against foreseeable risks. There was evidence that the framework of controls were substantially being complied with and the risk management process was considered to be good. Only minor errors or omissions were identified.

The following recommendations where agreed with Management to address the areas where controls enhancements could be made. This relates to risk 8.

Agresso:

I. The number of 'super users' should be reviewed and reduced to a more appropriate level subject to the departmental operational needs.
II. Internal IT and external remote 'super user' profiles to be deactivated and only reactivated for the short duration of specific projects
III. Tandridge District Council 'super users' profiles to be restricted to Tandridge data only to prevent access to Sevenoaks data.
IV. Activity reports to be produced regularly for all 'super user' profiles to monitor unusual or unexpected activity such as profile access set up, password changes, profile changes, system activity outside of expected 'day to day' role responsibilities to mitigate and reduce the risks of unauthorised activity.

Members will be advised of the progress in implementing these recommendations in due course.