APPENDIX 4

AUDIT REPORTS WITH MODERATE OR LOW LEVEL OF ASSURANCE ISSUED QUARTER 4 2017/18

PARIS Income Management – 26 March 2018

1 **Introduction**

1.1 In accordance with the Audit Plan for 2017/18 an audit review of the PARIS Income Management application has been completed. This report presents the findings and conclusions drawn from the audit for information and action where appropriate.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and co-operation received during the audit.

2 **Background**

2.1 The PARIS application is used for cash receipting and to process and reconcile payments from multiple departments across the Council. This review of the system and its supporting controls was performed in order to provide assurance that there are no data security or application control weaknesses in the ICT security and management of the application.

3 **Scope and Objectives of the Audit**

3.1 The work included a review of application security, incorporating access rights and privileges, audit trails, system administration functions, application support, and data backup.

3.2 Testing was performed to confirm that controls identified have operated as expected with documentary evidence being obtained where possible, although some reliance has had to be placed on verbal discussions with relevant staff.

3.3 The audit was designed to assess and provide assurance on the following risks:

- Non-compliance with current policies and procedures
- Application availability / data integrity is impaired in the absence of sufficient application security controls
- Inappropriate accesses allowed to system functionality and / or data
- Users have access to data / information not applicable to roles and responsibilities
- Users are not removed when they leave, or access privileges are not changed when roles / jobs change
- High level and super user functions are not properly managed

- System and data backups are not properly carried out.

4 Findings

4.1 Recommendations from Previous Report

4.1.1 The current position in respect of the recommendations from the audit reported in November 2012 is as follows:

Recommendation	Management Response	Current Status
1 The ICT team should confirm why the vendor for Total is provided with SYSADMIN access at instance level.	Remove sysadmin rights from TASK and warwickdc\consilium.	Completed.
2 A procedure should be implemented for regular purging of income transaction import files in the PARIS working directory.	The feasibility of the recommendation will be investigated and implemented if practical.	Due to staffing changes, management were unsure whether this had been actioned. The recommendation is, therefore, repeated in the action plan for this audit.
3 The feasibility of locking down the income transaction import files in the PARIS working directory against access through Windows navigation tools should be investigated.	Northgate have been consulted and they have been provided the necessary information. Application Support have started the required changes.	Completed – working directory files are no longer accessible through Windows.
4 Enquiries should be made with Northgate as to whether the scope of audit logging in the version of PARIS being considered for migration includes parameter changes.	Northgate have been consulted. The audit logging of parameter changes in version 41 of PARIS.	Completed. Management have since upgraded to a newer version of PARIS.

	5 Logging and reporting of parameter changes should be implemented, either as part of the envisaged upgrade or installation of the applicable system release previously produced as appropriate.	We will be upgrading to version 41 of PARIS as soon as possible.	Completed. Management have since upgraded to a newer version of PARIS.

4.2 **Policies & Procedures**

4.2.1 Key ICT policies and procedures relevant to application security, user administration and data backup and recovery were identified and obtained during the review. These were used in the process of reviewing the suitability of the controls in place for the PARIS application.

4.2.2 The policies identified as being of particular relevance in this review are the Information Security and Conduct Policy, Monitoring Policy, Software Policy and the Data Handling Policy.

4.3 **Application Security**

4.3.1 Authentication to the PARIS application is performed at the application level, with users being provided with password credentials that they are required to change on initial login.

4.3.2 It was found that strong passwords were enforced at the application level, as required by the Council's Information Security and Conduct Policy. Passwords are required to contain a capital alphanumeric character, a numeric character and a special character (such as @,$ or #). In addition the password itself must be a minimum of seven characters.

4.3.3 An audit trail of user activities is captured within the application, and reporting is available for review in the event of any suspect activity.

4.4 **Access Control**

4.4.1 It was noted that at the time of review ownership and responsibility for administration of the PARIS system was undergoing a period of change following the departure of the previous system owner, and that consequently there was a need to improve and / or formalise some of the supporting administration activities and controls.

4.4.2 Access to the application is currently provided by the Systems Officer, who has also recently been nominated the primary point of contact for support issues in relation to the system.

4.4.3 It was noted that requests for access to the application, or changes to existing users' access permissions, are made via a standard email rather

than through the use of a user request form.

4.4.4 Rather than specifying the access individuals require in the system, or specifying a particular role based permission, managers generally nominate an existing member of staff to base the new starter's permissions on. It was also found that there is no explicit requirement that a record of user requests / changes to a user's access permissions is retained.

Risk

Users may have systems access not applicable to their roles and responsibilities.

Recommendation

Management should formalise the user request process via the use of a user request form, to be used when requesting new users or changes to existing users access permissions. Forms should be retained to provide assurance that appropriate access rights have been granted to users according to their job role.

4.5 **User Roles & Responsibilities**

4.5.1 Access permissions are assigned to users via the use of roles and groups within the PARIS application. It was noted that there are a large number of role profiles and groups but that there is no supporting documentation / notes clearly describing what access privileges within the application are assigned to each role / group.

Risk

Users may be assigned inappropriate access permissions.

Recommendation

Management should consider documenting the role profiles in order to gain better visibility of the access rights assigned to each role and provide further assurance that the correct level of access is being assigned to users.

4.5.2 Although accounts are reviewed on an ad-hoc basis, there is currently no regular exercise undertaken to review and verify that users' access levels within the application are appropriate i.e. that no users have been granted a high degree of access in error or that users have been able to retain and 'collect' access rights following a change of job role.

Risk

Users may be granted access permissions above and beyond that required by their job role.

Recommendation

A regular, at least annual, exercise should be undertaken to review users' access permissions within PARIS to ensure they remain appropriate.

4.6 **Leavers Process**

4.6.1 It is the responsibility of the leaver's team manager to notify ICT of leavers via the use of a leaver form, in order for a user's network and application accounts to be disabled. In the event that this form is not completed it is possible for accounts to remain active. It was found that the Systems Officer has additional controls in place to identify and remove leavers' accounts.

4.6.2 These controls include a process of comparing HR leaver data against live user accounts on a monthly basis and removing any leaver accounts identified, effectively mitigating the risks around leavers not being reported and removed from the system in a timely manner.

4.7 **High Level & Superuser Functions**

4.7.1 Administrator access rights, including the ability to create and delete users, are granted to a limited number of approved users. A list of the members of this group was obtained and reviewed with management during the review and it was confirmed that each user required this access and had the appropriate level of access for their job role.

4.7.2 A review of high privilege PARIS user accounts identified the existence of an active administrator level account named 'Administrator'. Although it is understood this account is unused and that ICT staff use named individual accounts for administration purposes it is possible the account could be used maliciously, or in error, to perform activities that cannot be easily traced back to an individual.

Risk

There may be a lack of accountability with the audit trail of actions performed showing the use of a generic administrator level account.

Recommendation

The purpose of the 'Administrator' account should be investigated and, if possible, the account should be renamed or deleted in order to remove the potential for misuse.

4.8 **Database Security**

4.8.1 Database security controls including authentication requirements, logging settings, and use of default / generic accounts were reviewed using the Microsoft Baseline Security Analyser (MBSA) tool, with scans of key PARIS servers performed and reviewed for potential security issues.

4.8.2 It was noted as part of this exercise that the SQL instance relating to the application uses 'Mixed Mode' authentication, rather than using Windows authentication (which would provide improved security). It was found that this is required by the application supplier as part of their support arrangements and that a change could have an adverse impact of the system operation and could not be easily altered. This has, therefore, been raised to highlight the security level but not as an issue to be resolved.

4.9 Backup & Recovery

4.9.1 Backups of the PARIS servers and database are made using HP Data Protector. Daily backups are made each night and kept in the onsite tape library for two weeks.

4.9.2 Backups are performed over the weekend and include all systems. The weekly tapes are taken by a member of the Infrastructure team to be stored off-site at the Town Hall where they are kept for a four week period. Monthly full backups are also made and taken off-site on a monthly basis. These are retained for six months.

4.9.3 It was found that, whilst regular backups are made and retained, there has been no testing of the ability to restore PARIS data from backups that management are aware of.

Risk

There may be limited or no assurance that the application can be recovered within an acceptable timescale and that potential issues have been identified and addressed.

Recommendation

Testing of PARIS should be scheduled as part of the next disaster recovery testing exercise. The testing should be documented and include the time taken to recover systems and services, whether recovery time and point objectives have been met and include detail on any issues and actions arising from the testing.

5 Conclusions

5.1 The audit identified three medium and three low rated recommendations, giving a MODERATE level of assurance around the application security of the PARIS application.

5.2 The assurance bands are shown below:

Level of Assurance	Definition
Substantial Assurance	There is a sound system of control in place and compliance with the key controls.
Moderate Assurance	Whilst the system of control is broadly satisfactory,

	some controls are weak or non-existent and there is non-compliance with several controls.
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

6 **Management Action**

6.1 The recommendations arising above are reproduced in the Action Plan for management attention.

Banking Arrangements – 1 February 2018

1 **Introduction**

1.1 In accordance with the Audit Plan for 2017/18, an examination of the above subject area has been undertaken and this report presents the findings and conclusions drawn from the audit for information and action where appropriate. This topic was last audited in June 2014.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and cooperation received during the audit.

1.3 It is acknowledged that the Principal Accountant responsible for the day-to-day operation and administration of bank accounts was relatively new to the post at the time of the audit and has subsequently left the Council. Therefore, the opportunity to review processes and initiate and implement improvement has been significantly limited.

2 **Background**

2.1 The Council's banking arrangements help ensure that money is held in safe and profitable organisations. This has a direct impact on the Council achieving the Money theme of the Fit for the Future (FFF) strategy, specifically around the internal intended outcomes of achieving better returns and better use of our (financial) assets.

2.2 The current contract came into effect on 1 March 2015 for a period of five years at a cost of approximately £25,000 per year.

3 **Scope and Objectives of the Audit**

3.1 The objective of the audit was to test the key controls relevant to the current banking arrangements, including controls over the posting of transactions and the security of on-line transactions.

3.2 The audit covered the following control objectives:

- A control framework has been established for banking arrangements and bank reconciliations, including tendering arrangements, statement of responsibilities, written statement of bank terms and fidelity guarantee policy.
- Documented procedures for all banking related processes are in place and available to all relevant staff.
- All payments/debits from the bank accounts are properly authorised and processed accurately and completely to the ledger.
- Bank statements are regularly reconciled to the ledger (both income and expenditure) and interest and charges are accurate and in line with the agreed terms.
- Transaction volumes (which give rise to the charges) are reviewed.
- An appropriate bank mandate is in place for all bank accounts.
- Cheque stationery is appropriately controlled.
- Presented cheques are verified to the payments system.
- Computer systems are appropriately secured and business continuity arrangements are in place to ensure that business critical interactions with the bank can continue independently of Council systems as far as possible.
- On line payments require appropriate authorisation.
- Suspense accounts are regularly reviewed and reconciled by an independent officer.

4 Findings

4.1 Recommendations from Previous Report

4.1.1 The current position in respect of the recommendations from the audit reported in June 2014 is as follows:

Recommendation	Management Response	Current Status
1 The Code of Financial Practice should be updated on the Council's website, as per the amendment approved by Executive.	The website version of the Code of Financial Practice will be updated to include the amendment.	Reviewed, updated and approved by Council in April 2015. Not reviewed since as no changes. See 4.2 (Control Framework).
2 Interest received on the Business Deposit Account should be checked to the Council's own calculations on a quarterly basis to ensure that any discrepancies noted can be queried in a	The actual interest credited to the BDA will be checked against our spreadsheet and any significant discrepancy reported to the bank.	All accounts are subject to quarterly review, including interest received and charged. See 4.13 (Bank Charges).

timely manner.		
3 The old cheque stock should either be used (if they are still valid cheques) or be securely destroyed.	The old cheque stock does not contain valid cheques and can no longer be used; each box has been clearly marked with an "X" to ensure that they are not issued and they are stored on the top shelf of the cabinet separate to the current valid stock. However, arrangements will be made to ensure that the old stock is securely disposed of / destroyed to remove all risk.	Completed.

4.2 **Control Framework**

4.2.1 The Constitution, approved by Council on 25 January 2017, includes at Section 4, the Scheme of Delegation. Section 6 F(13) ii, states that the Head of Finance and Chief Finance (S151) Officer shall have authority to, "make such banking arrangements, including opening of banking accounts, as appear necessary for the proper management of the Council's finances".

4.2.2 The Code of Financial Practice, includes at Section 7, Banking Arrangements and Treasury Management. Section 7.1 states that, "the Head of Finance is responsible for all arrangements with the Council's bankers.

4.2.3 Further to this, the Treasury Management procedures detail the operation of bank accounts. However, a review of these found that they deal exclusively with investments.

4.3 **Procedure Documentation**

4.3.1 Internal Audit was informed that there are no documented procedures for the operation of the PARIS system.

4.3.2 In addition, there is no single procedure manual that would cover all aspects of the banking functions performed within Finance. Instead, individual staff members have drawn up their own guidance notes for their parts of the processes, which would be available to others if required.

4.3.3 Furthermore, it was confirmed that there are no documented step by step process notes or guidelines for the reconciliation process (see 4.5 below), the maintenance of the bank mandate (see 4.7 below), or for managing access to HSBC.net (see 4.9 below).

Risks

Without documented procedures and guidelines, inadequate, inefficient or out of date processes may develop.

Knowledge of processes may be lost should current staff leave the Council.

Recommendation:

A full set of documented procedures for the Council's banking arrangements should be drawn up to provide step by step instructions and guidelines for the relevant processes. This is particularly important in developing succession planning arrangements, including knowledge retention.

4.3.4 Procedures for HSBC.net are available online but these can also be downloaded.

4.4 **Payments and Debits**

4.4.1 All payments/debits from the account are properly authorised and processed accurately and completely to the financial ledger.

4.4.2 A sample of payments was selected from the bank statements and testing confirmed that all payments had been:

- requested by staff from the relevant department;
- accompanied by a Priority Payment form that was completed by a member of staff from the Accounts team;
- checked and authorised on HSBC.net by the Principal Accountant or another senior member of Finance staff; and
- reconciled to the ledger.

4.4.3 The bank reconciliation process ensures income received is accurately processed to the ledger.

4.4.4 Expenditure items are authorised prior to being incurred and again, the bank reconciliation process ensures the expenditure on the ledger matches that at the bank.

4.5 **Reconciliation**

4.5.1 The Accountancy Assistant (Bank Reconciliation) undertakes the monthly bank reconciliations. There are some old process notes but these are not used and do not cover the entire process (see 4.3.3 above).

4.5.2 Bank statements are downloaded from HSBC.net on a daily basis, by logging in to the online facility. Although these are reviewed daily, the actual formal reconciliations are undertaken each month.

4.5.3 Spreadsheets have been created to facilitate the reconciliation and entries are manually input from the statements and then from the cashbooks on the Council's general ledger.

4.5.4 Testing was undertaken to check the frequency and accuracy of the reconciliations for both income and expenditure.

4.5.5 It was established that these are undertaken each month, but on a year to data basis rather than a full reconciliation of the monthly bank transactions to the monthly ledger movements. Therefore, it was not possible to reconcile the bank statements to the income or expenditure as the opening balances on the statements were for the actual month and the ledger totals were year to date.

Risk

Monthly movements may not be tracked and reconciled to the Council's ledger.

Recommendation:

The reconciliation process should include a monthly summary reconciliation position that shows the actual monthly bank statement movements, compared to the ledger and actual cashbook movements, with a list of the transactions making up the reconciling difference including reasons.

4.5.6 It was also identified that the bank reconciliations are not subject to independent review and sign off.

Risk

Errors and discrepancies may go unnoticed.

Recommendation:

All bank reconciliations should be subject to independent review and sign off to ensure timeliness and that any errors, discrepancies and unexplained differences are highlighted and investigated.

4.5.7 Income received at the Royal Spa Centre is processed using a system called OLR2, which is part of the PARIS income system. However, there have been issues with this system and a lack of understanding resulting in income being banked but not being input to the ledger.

4.5.8 It was established that the previous Principal Accountant was aware of this issue and undertook a separate monthly reconciliation to identify and correctly post the income received via OLR2. This was a 'work around' solution rather than a system fix. However, the current Principal Accountant and the existing team are not aware of the process for this or why the income is not automatically posted.

Risk

Income may be incorrectly processed.

Recommendation

An investigation should be undertaken of the use of the OLR2 system at the Royal Spa Centre to establish why income received is not posted to the ledger.

Where a 'work around' solution is used, the process should be documented and retained for continuity purposes. However, this should only be used on a temporary basis until a permanent solution is introduced.

4.6 **Transaction Volumes**

4.6.1 It was identified that a Schedule of Rates was detailed at the tender evaluation stage (for the current contract) and these were subsequently agreed.

4.6.2 Schedule 6 of the agreed contract (see 4.12 below) detailed the final schedule of rates along with the agreed annual transaction volumes, including:

- Direct Debits paid – 385; charge £15
- BACS items – 556,035; charge £5,560

4.6.3 These figures were based on the volume of transactions during the year ended 31 December 2013. However, the rates have not been reviewed since the start of the contract and no one at the Council undertakes an annual review of transaction volumes.

Risk

The Council may be overcharged.

Recommendation:

An annual review of transaction volumes should be undertaken to ensure they are still within the agreed volumes included within the Schedule of Rates and the rates are, therefore, still appropriate.

4.7 **Bank Mandate**

4.7.1 The bank mandate was reviewed and it was confirmed that the listed staff were appropriate and current.

4.7.2 The Principal Accountant is responsible for maintaining the mandate but was not aware of the process to add to or remove a member or staff from it, as there was no documented procedure or guidelines. It is recommended that this is included in the new procedure documentation (see 4.3.3 above)

4.7.3 It was identified that when the previous Principal Accountant retired, the Assistant Accountant (Capital and Treasury) prepared a letter for the bank to remove him from the mandate and include the replacement, with the letter being signed by the retiring member of staff.

4.8 **Cheque Payments & Security**

4.8.1 There are twice weekly cheque runs, for which the Corporate Support team (CST) is responsible for. All cheques are batch printed and the stock of cheques is retained in a locked safe in the CST office, to which only CST staff have access.

4.8.2 A log of cheques is retained and when a payment run is undertaken, the number of cheques and the first and last cheque numbers are recorded. Testing established that there are no gaps in the log.

4.8.3 Cheques are ordered from HSBC by the Media team, who retain a log of all cheques. These are collected by CST staff who are required to sign for the cheques.

4.8.4 Un-presented cheques listings are regularly reviewed by the Accountancy Assistant (Bank Reconciliation) as part of the monthly expenditure reconciliation. These are then monitored on a daily basis, when the bank statements are downloaded.

4.8.5 If the cheques are not presented in time they are cancelled.

4.9 **IT Systems – HSBC.net**

4.9.1 Access to HSBC.net is assigned according to job role and need to use.

4.9.2 A list of current active users was obtained and it was confirmed that all users were current.

4.9.3 Responsibility for the administration of the process was found to lie with the Principal Accountant, who will shortly be leaving the Council. However, there is no documented process.

4.9.4 A sample of payments was selected for testing and it was confirmed that authorisation via HSBC.net was appropriate and in line with that of cheque payments.

4.9.5 The review of the reconciliation process (see 4.5 above), confirmed that bank statement information is downloaded from HSBC.net on a daily basis by the Accountancy Assistant (Bank Reconciliation).

4.10 **Online Payments**

4.10.1 A sample of online payments was selected for testing to ensure that the system requires (at least) the same levels of authorisation as cheques.

4.10.2 It was established that payments require one user to prepare the paperwork and then two authorisers to check and authorise the payment on the system. The authorisers check that the sort-code, account number, payee and amounts are correct and that the payment request is above-board.

4.10.3 The testing confirmed that, in all cases, payments had been independently requested by staff from the relevant department, or was included on a payment schedule or remittance, sent to the Accounts team.

4.10.4 In addition, a Priority Payment form had been completed by a member of staff from the Accounts team and checked and agreed by the Principal Accountant.

4.11 **Suspense Account Reconciliation**

4.11.1 There is a suspense account, where unidentified credit transactions are processed to. The account details are downloaded on a daily basis by the Accountancy Assistant (Bank Reconciliation) and the amounts are cleared where possible.

4.11.2 Details (including those of the transfer) are printed and retained on hard copy files. The files and the suspense account were reviewed which confirmed that the transactions are being reviewed and cleared and that there were no long-standing items.

4.12 **Agreement with the Bank**

4.12.1 A formal tender process was undertaken during 2014 and HSBC was awarded the contract to provide banking services to the Council.

4.12.2 The contract, which is for an initial five-year period with an option to extend for a further five years, was signed by all parties in February 2015 and commenced on 1 March 2015. This was confirmed by review of the hard copy signed contract.

4.12.3 The original signed contract (which was reviewed) is stored securely in the document store.

4.13 **Bank Charges**

4.13.1 We established that interest received and bank charges for all bank accounts are reviewed on a quarterly basis by the Assistant Accountant (Capital & Treasury).

4.13.2 However, the interest and charges are not specifically checked and agreed to those agreed, only that if the amount appears to be higher than normal on the bank statement, then it would be reviewed and investigated.

Risk

The Council may be incorrectly charged and may not receive the correct interest.

Recommendation:

Interest received and charged should be reviewed to ensure it is in line with the agreed rates.

5 Conclusions

5.1 Following our review, in overall terms we are able to give a MODERATE degree of assurance that the systems and controls in place in respect of Banking Arrangements are appropriate and are working effectively.

5.2 The assurance bands are shown overleaf:

Level of Assurance	Definition
Substantial Assurance	There is a sound system of control in place and compliance with the key controls.
Moderate Assurance	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

5.3 Issues were identified relating to:

- The lack of procedure documentation.
- The bank reconciliation processes and reviews of completed reconciliations.
- Income not being recorded on the financial ledger.
- The lack of an annual review of transaction volumes.
- The checking of interest received and charged against the expected rates and amounts.

6 Management Action

6.1 The recommendations arising above are reproduced in the Action Plan for management attention.

Flood Risk Management – 31 March 2018

1 Introduction

1.1 In accordance with the Audit Plan for 2017/18, an examination of the systems and procedures in place for dealing with Flood Risk Management (FRM) has been undertaken and this report presents the findings and conclusions drawn from the audit for information and action where appropriate.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and cooperation received during the audit.

2 Background

2.1 The last audit of FRM, which was also the first audit undertaken on the subject, was completed in November 2014.

2.2 At that time most of the related systems and procedures were contained within the Environmental Sustainability Team in Health and Community Protection (H&CP) and the majority of the work was undertaken by two engineers.

2.3 Since that time as a result of various restructures and redesigns the council currently has no engineering resource and the work previously undertaken in H&CP has been distributed to other service areas, mainly Neighbourhood Services and the Assets Team in Chief Executive's, and to the County Council.

3 Scope and Objectives of the Audit

3.1 The audit was undertaken to test the management and financial controls in place.

3.2 In terms of scope, the audit covered the following areas (overleaf):

- There are appropriate management, structural and operational procedures in place to deal with the risk of flooding.
- The council's legal obligations are being complied with.
- All watercourses on council land are identified, recorded and maintained.
- Proposed developments in the district are referred to WCC for flood risk implications.
- Work is ordered in accordance with the Code of Procurement Practice.
- Work carried out for WCC is covered by a formal agreement.
- Corporate budgetary control procedures are being followed.
- The risks associated with the service are identified, recorded and managed.

3.3 The audit programme identified the expected controls. The control objectives examined were:

- Responsibility for FRM is clear with established procedures in place.
- The council's legal obligations are being complied with.
- Watercourses on council land are inspected and maintained.
- All watercourses and trash screens are detailed both in narrative and on maps.
- Details of work to be undertaken are supplied to the contractor.
- Relevant planning applications are referred for possible flooding implications.
- Tenders are invited for work and contracts are in place.
- Work undertaken for the County Council is covered by a suitable agreement.
- The County are billed in advance for the work.
- Budgets are controlled in line with standard procedures.
- Relevant risks are identified, recorded and managed.

4 Findings

4.1 Recommendations from Previous Reports

4.1.1 The last report on Flood Risk Management was issued on 27 November 2014 and it contained a number of recommendations. The response at the time and the current position are detailed in Appendix A.

4.1.2 In respect of those previous recommendations, the completely different management arrangements that are now in place, the budgetary structure and staffing issues have rendered the recommendations from the last audit redundant. This will be explained below.

4.2 Overall management of FRM

4.2.1 At the time of the last audit there were two Engineers posts in H&CP and they dealt with virtually all matters relating to FRM. One post was closely involved in a flood alleviation capital scheme that was taking place at the time and the other post managed the routine inspection and maintenance work and dealt with referrals from Development Management on planning applications.

4.2.2 Now H&CP have virtually no responsibility for FRM and there are no Engineers posts in the current structure. The routine inspection and maintenance aspects for watercourses and trash screens are dealt with in Neighbourhood Services, the Assets Team in Chief Executive's deal with the maintenance of pumping stations and would manage any capital schemes and under an SLA the County Council are consulted on planning applications and drainage matters.

4.2.3 The Environmental Protection Team in H&CP have held the budget for the payment of the SLA with the County but as from 2018/2019 this is being transferred to Development Management.

4.2.4 Partway through the audit comment was made that the approach being adopted was akin to a contract management audit and that a wider view of managing the risk should be taken to include the issues surrounding Sustainable Urban Drainage Systems (SUDS). Up to this point there had been no intention to consider SUDS as part of the audit due entirely to the fact that SUDS was a completely alien term and so not included in the audit programme. Given the nature of the concerns expressed about SUDS, the fact that the audit was already in progress and that there simply wouldn't be time to consider the matter to any meaningful degree it was suggested that the matter would be examined in a fairly broad fashion with any recommendation being in a similar vein.

4.2.5 Some brief investigation and explanation revealed that SUDS are a system whereby surface water in urban areas is stored temporarily thereby reducing the flow into local watercourses which otherwise might result in flooding. The Local Plan requires that all new major developments must incorporate SUDS.

4.2.6 Discussions took place with a number of officers about SUDS and it soon became clear that there was a good understanding of what they were and of the issues associated with them. Most officers expressed concerns that could be summarised as a lack of preparedness for dealing with them which might result in serious problems in the future. There may only be a limited number around at the moment but the development of the District in the Local Plan suggests that a lot more will appear over the life of The Plan.

4.2.7 Several comments referred to the council's lack of experience in dealing with SUDS and the lack of the necessary in house expertise to advise on their suitability and fit for purpose. What currently happens with planning applications for major developments is that among the conditions for approval will be a condition that a SUDS must be installed. In time the developer submits proposals to fulfil the condition and these are forwarded to the County Council for their approval.

4.2.8 When the scheme has been completed it will be handed over to the council for adoption. What is unclear at that stage is whether or not the SUDS has been provided in accordance with the proposals approved, if it is fit for purpose, if it has been provided to an appropriate standard and if, as part of the financial settlement, there are sufficient funds to meet the ongoing maintenance costs.

4.2.9 In the course of discussions some officers cited the council's lack of in house engineering resources as being a factor in the general management of SUDS. Admittedly there are no engineering posts in H&CP as there were at the time of the last audit but engineering resources are provided to the council under the SLA with WCC. It was claimed that the value of the previous engineering posts was overstated as a result of a misunderstanding in Service Areas of what the engineers actually did against what people thought they did.

4.2.10 There is, however, an Engineer's post on the establishment. As part of the restructure of H&CP that was reported to Employment Committee in March 2017 a post of Engineer was deleted and a post of Engineer (0.6fte) was created. The new post is located in the Assets Team. No progress has been made with filling the post possibly because the Team is currently undergoing a redesign. When the post will be filled and what the duties will be are also not clear.

4.2.10 In summary there are a lot of concerns surrounding SUDS which are mainly around their quality or fitness for purpose and the funding of their maintenance. It would seem that the inevitable expansion of their use is not being managed in a coordinated fashion.

Risks

SUDS that are not fit for purpose might be installed which may increase the risk of flooding.

Funds deposited by the developer may not be sufficient to meet ongoing maintenance costs.

Recommendation

A coordinated approach to managing the expansion of SUDS in the District should be adopted by involving all relevant senior managers to identify the potential problems and to propose solutions.

4.3 **Legal obligations are being complied with**

4.3.1 There are a number of Acts of Parliament that a local authority needs to comply with in respect of land, water and flooding with the main one being the Land Drainage Act 1991. The Act requires that a watercourse is maintained by its owner in such a condition that free flow of water is not impeded. The council also has powers of enforcement on other landowners if they fail to meet their duties. The council has powers to serve a notice and if it is ignored to carry out the necessary work and recharge the owner.

4.3.2 Watercourses, brooks and streams, on council land are inspected and if necessary blockages and debris are removed through a planned maintenance programme undertaken by one of the council's main contractors.

4.3.2 The work is specified in the Grounds Maintenance contract and monthly reports of inspections undertaken and the condition of the watercourses are submitted to Contract Services.

4.4 **All watercourses are identified and maintained**

4.4.1 The watercourses that are on land owned by the council are all recorded on both lists and maps. A copy of the maps is held in Contract Services and a copy has been supplied to the contractor.

4.4.2 Under the terms of the contract the contractor is required to inspect all watercourses monthly and to remove any blockages that will impede the free flow of water. Anything removed must be taken to the tip for disposal.

4.4.3 The trash screens to be cleared are all referenced and listed and the contactor is required to remove all debris on either a four or eight weekly basis. The cost of this work is recovered from the County Council.

4.5 **Proposed developments are referred for flood risk implications**

4.5.1 At the time of the last audit a list of planning applications validated each week was forwarded to H&CP for observation and comment on any flood risk implications. In some cases the design and construction of the development was considered as well as the proposed location. The work was mainly undertaken by one of the engineers.

4.5.2 The work is currently outsourced and undertaken by the Warwickshire County Council Flood Risk Management Team under an agreement that runs from year to year until terminated by either party giving notice.

4.6 **Work is ordered in accordance with the Code of Procurement Practice**

4.6.1 Another change since the last audit is the way that maintenance work is ordered. There was an issue last time in that maintenance work was carried out by an outside contractor to a value of around £40,000 a year and there was no market testing and no contract. A recommendation was made that the procurement process should be followed and tenders should be invited.

4.6.2 The response at the time (November 2014) was that tender documents would be prepared to enable a contract to start in April 2015. Due to the workload of the Procurement Team this date was extended to April 2016. What happened next wasn't established partly due to the fact that the people involved at the time no longer work for the council and partly because of the way that work has been undertaken since April 2016.

4.6.3 The work involved in inspecting and clearing watercourses and inspecting and clearing trash screens has been incorporated into the Grounds Maintenance and Street Cleansing contracts respectively. Why this decision was taken and whether or not it bends the Procurement rules wasn't established. The rates charged by the contractors look to be at a level where they make very little from the deal and it is hard to imagine that they could be bettered.

4.7 **Work for WCC is covered by an agreement**

4.7.1 Part of the work on FRM involves the clearance of trash screens on behalf of the County Council. Trash screens are large metal grids that prevent large items of debris entering a watercourse at the point where it disappears from view which is usually into a culvert.

4.7.2 The last audit of FRM unearthed a draft agreement dating back to 2004 that set out in broad terms how the arrangement would operate both in terms of the work to be undertaken and how WCC would make payment. The agreement was never enacted.

4.7.3 What there was instead and what amounted to an agreement was an exchange of emails between the County and H&CP which only concerned the amount that the County would be paying for the work. In the context of the work being undertaken and dealing with another local authority the informal nature of the "agreement" was seen as acceptable and low risk and there was no recommendation that a more formal relationship should be established.

4.7.4 Currently the work on trash screens and the recovery of the cost of the work plus the council's administration costs from WCC is managed by Contract Services. At the moment the absence of certain key staff in Contract Services has created something of a knowledge gap and how much the County are going to pay for 2017/18 is unknown and consequently no sundry debtor invoices have been raised. The matter is currently being pursued and the County have been asked to submit orders for the work so that invoices can be raised.

4.8 **Budgets are controlled in line with standard procedures**

4.8.1 Budgets for FRM work which were previously all managed by H&CP have now been distributed among a number of other service areas but corporate budgetary control will still apply in that a specific officer will be identified as being responsible and regular monitoring will take place.

4.8.2 Recent budgetary performance (current and previous years) over the various cost centres was examined and there was nothing untoward.

4.8.3 The cost of watercourse inspection and maintenance is part of the Grounds Maintenance budget and is not separately identified. The work on trash screens forms part of the Street Cleansing contract and is paid for accordingly. As part of reviewing the budget the cost of the trash screen work is transferred annually to its own cost centre and forms the basis of the recovery from the County.

4.8.4 The budget for Alleviation of Flooding now appears in the Chief Executive's service area and is the responsibility of the Interim Asset Manager. For 2018/19 it includes a recharge from what is described in the budget book as Environmental Health Services of £102,700. This is the level of recharge that would have applied when H&CP had two engineers in post spending most of their time on flooding related matters. It is inappropriate in the present circumstances and no doubt it will be corrected at revised estimate time.

4.9 **Risk management**

4.9.1 Although the council has a role to play in managing the risk of flooding and an even greater role in responding to a major flooding incident, its influence and options are limited to the activities described in the report. The

council's role is relatively minor in comparison to that of the Environment Agency and the County Council.

4.9.2 Some of the service area risk registers and the Significant Business Risk Register make some specific minor reference or some indirect reference to flooding and climate change. In many ways as a major flooding incident would be down to the forces of nature the risk would be impossible to manage.

4.9.3 As this audit is about how the council manages the risk of flooding the main risk is in not being able to carry out that function i.e. having all of the usual resources such as staffing, systems, accommodation and communications etc. to deliver the service. Every risk register includes the generic risks.

5 **Conclusions**

5.1 Following our review, we are able to give a MODERATE degree of assurance that the systems and controls in place for Flood Risk Management are appropriate and are working effectively.

5.2 The assurance bands are shown below:

Level of Assurance	Definition
Substantial Assurance	There is a sound system of control in place and compliance with the key controls.
Moderate Assurance	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

6 **Management Action**

6.1 The recommendations arising above are reproduced in the Action Plan for management attention.

Information Governance: Preparations for General Data Protection Regulations – 9 March 2018

1 **Introduction**

1.1 In accordance with the Audit Plan for 2017/18 a review of the forthcoming General Data Protection Regulations (GDPR) under the Audit Plan umbrella of Information Governance has been completed. This report presents the findings and conclusions drawn from the audit for information and action where appropriate.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and co-operation received during the audit.

2 Background

2.1 The purpose of the audit was to ensure that the Council is adequately prepared for the forthcoming changes to the General Data Protection Regulations. This change is due in May 2018.

2.2 The EU General Data Protection Regulations will affect every organisation that processes the personally identifiable information (PII) of EU residents. The introduction of the GDPR represents the most significant change to data protection law in the UK, EU, and globally, in recent years. Every organisation must be aware of the requirements of the GDPR as we are now in the transition phase leading up to May 2018.

2.3 Key to the new regulations will be an increase to the rights of data subjects who will have a greater influence on how their data is processed. Other significant areas of change include the rules on consent and the requirement for a dedicated data protection officer role. The Regulation also mandates considerably tougher penalties for data breaches than under the current law, from a theoretical maximum of £500,000 that the ICO could levy under current legislation (in practice, the ICO has never issued a penalty higher than £400,000), penalties under GDPR have an upper limit of €20 million (approx. £17million) or 4% or annual global turnover, whichever is the higher.

2.4 At the time of the audit, the Council was in the process of appointing a Data Protection Officer (DPO). This post will be a shared role with Stratford on Avon Council. The recruitment process has meant that the process of addressing GDPR within the Council had been put on hold until the expertise that the new post will bring becomes available.

3 Scope and Objectives of the Audit

3.1 The audit was an assurance review of the information governance arrangement in light of the legislation changes in 2018. There was an advisory element to provide some guidance as to the likely impact on technical controls which the new Act imposes.

3.2 Because of the 'in limbo' status of this process, limited testing has been possible. Some work has commenced but has halted until the new DPO is in post and can analyse the prevailing arrangements and make the necessary changes. Such testing as was possible has been performed to confirm that controls identified have operated as expected with documentary evidence being obtained where possible, although some reliance has had to be placed on verbal discussions with relevant staff.

3.2 The audit scope included:

Information management (policies, ownership, asset categorisation).
Information-sharing arrangements.
ICT technical requirements, if clear and known.

4 Findings

4.1 Recommendations from Previous Report

4.1.1 This section is not relevant as this is the first audit of this area.

4.2 GDPR Management Arrangements

4.2.1 Essentially this involves the requirement for a dedicated Data protection Officer (DPO) role. At the time of the audit, this role did not exist but was being recruited. It is planned that a shared resource (with Stratford on Avon) will be appointed. In the meantime, the responsibilities were being covered by Graham Leach, the Council's Democratic Services Manager and Deputy Monitoring Officer. The Data Protection Officer role will be the key coordinator of the activities necessary to promote the awareness and lead the compliance preparation activities. Although this key control was not in place at the time of the audit, it was clearly being addressed therefore no recommendation has been made. However, the relatively late appointment and the planned (part-time) resource allocation might be insufficient in the short term to ensure that the Council has the necessary compliance arrangements in place by the May 2018 deadline.

4.2.2 There are aspects to GDPR management that would normally fall within the responsibility of a DPO. These include Policy and procedure development, awareness raising, training. The former is dealt with elsewhere in this report, but the remaining two will need to have swift actions taken once the new DPO is in post.

Risk

Staff may lack awareness of the Council's and their own responsibilities.

Recommendation

A programme of targeted awareness raising events (workshops, short training courses/sessions, etc.) and updated communications for Council staff should be introduced at an early point once the new person is in post.

4.3 Information Management

4.3.1 We were informed during the audit that policies for IG had started to be drafted, but that this had been halted until the new DPO was in post.

4.3.2 There are a number of policies that may require amending to ensure GDPR

compliance. Specific IG (GDPR) policies, also information security and any associated policies (e.g. HR).

Risk

Policy documentation may be out of date and the Council is non-compliant.

Recommendation

A full review of all relevant policies and procedures should take place once the new officer is in post.

4.3.3 There is a requirement to ensure that information accountability is in place. This is a recurring theme in GDPR. This is not new but rather than being implicit, as in the Data Protection Act, GDPR emphasises its significance. This would normally be achieved by the introduction of information assets owners. This had yet to be implemented at the time of the audit. The new accountability principle in Article 5(2) requires the Council to demonstrate compliance with the principles and states explicitly that this is the Council's responsibility. The Council is expected to put into place comprehensive but proportionate governance measures.

Risk

Non-compliance with legislation.

Recommendation

An information audit should be undertaken and Information Asset Owners should be appointed (and trained as appropriate) as soon as practical.

4.3.4 A key element of GDPR is "data protection by default" which requires mechanisms to be in place within the Council to ensure that, as a matter of routine, only personal data which are necessary for each specific purpose are processed. This obligation includes ensuring that only the minimum amount of personal data is collected and processed for a specific purpose; the extent of processing is limited to that necessary for each purpose; the data are stored no longer than necessary and access is restricted to that necessary for each purpose. As part of a "data protection by design" approach, a data protection impact assessment (DPIA) will become a mandatory pre-requisite before processing personal data which is likely to result in a high risk to the rights and freedoms of individuals. The Council should consider how it will implement DPIAs for relevant personal data processing systems (e.g. Council Tax, Housing Benefits).

Risk

Non-compliance with legislation.

Recommendation

The Council should document and implement a procedure for Data Protection Impact Assessments (DPIA).

4.3.5 To assist with meeting Article 30 the Council will need to look closely at its Information Asset Register (IAR) process and undertake an information audit across all services to map data (items and flows). Based on our discussions, it was not clear whether or how up-to-date the services' IARs are.

Risk

Non-compliance with legislation.

Recommendation

A comprehensive information audit should be undertaken to formulate an Information Asset Register sufficient to meet the requirements of Article 30.

4.4 Information Sharing

4.4.1 To help comply with the GDPRs accountability requirements the lawful basis of processing should be fully documented along with any sharing requirement/partners. Where sharing is carried out, the IAR should provide a link to the information sharing agreement signed by all parties to the sharing. Under the GDPR, some individuals' rights will be modified depending on the lawful basis for processing their personal data.

Risk

Non-compliance with legislation.

Recommendation

The Council should review and /or introduce compliant information sharing agreements.

4.4.2 Articles 44 to 50 introduce new rules for transfers of data to other countries or international organisations. We did not identify such transfers during our discussions, however particular attention should be applied to any existing or future cloud service facilities / systems used or hosted solutions to ensure the system owners are fully aware of where the processing of Council data is taking place. This should be considered either during the information audit process (recommendation 4 refers), as part of new system acquisitions or as a separate focussed exercise and the guidance provided by the ICO followed where necessary. Future considerations should be addressed through the PIA / DPIA process. This is provided for guidance only – not an action point at this time.

4.5 **Technical Requirements**

4.5.1 Detailed information about the detailed technical security implications of GDPR are limited at the time of drafting this report. In addition, the GDPR Articles talk of "*implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk*". Our research has revealed little at this stage that specifically states, or provides exemplar information on which to draw. Our research shows that GDPR Article 32 describes the security of processing standards and this is where relevant information might be found. Article 32 states that those appropriate measures as mentioned above should take into account the "*state of the art*" (taken to mean the technologies at the Council's disposal), "*the cost of implementation"* and "*the nature, scope context and purpose of the processing"* as well as "*the risk…"*.

4.5.2 Article 32 identifies the following as the kinds of security actions that might be suitable to the risk:

- Pseudonymisation of personal data;
- encryption of personal data;
- confidentiality, integrity and availability of personal data
- resilience of processing systems;
- ability to recover and restore access to personal data in a timely manner in the event of an incident; and
- the introduction of a process that regularly tests and evaluates the effectiveness of controls and processes for ensuring security of processing.

4.5.3 Because GDPR does not describe specific technical measures to be used to secure personal data, means that this is left open to interpretation. Commentators are suggesting that the current legislation has set broad goals whilst the detail will be forthcoming in future updates. It is known that GDPR takes a risk-based approach to data security and confidentiality. The higher the risk, the greater the need (and therefore likely greater cost/effort) of the required solution.

4.5.4 Our research has revealed that Article 32, which replaces Principal 7 as the relevant standard, has actually changed very little in terms of content. It is therefore apparent that good quality, robust controls will be a strong starting point for compliance with GDPR in technical terms. There are other, external standards or guidance that will help in this regard. The ISO standard for Information Security Management (ISO27k) is relevant, as is the PCI-DSS compliance standard. This along with the Cyber Essentials Scheme guidance will provide very useful baselines of control for GDPR compliance. Compliance with these industry standards will also greatly increase the likelihood of compliance with GDPR.

4.5.5 It should be remembered that the above is about the processing and protection of personal information for GDPR compliance.

4.5.6 The ICT Audits undertaken in previous years will also be a source of relevant information in order to ensure good baselines of control; the

relevant ones were:

- Change Management (2016/17)
- Patch Management (2016/17)
- ITDR (2016/17)
- Total Finance – Application review (2016/17)
- Civica – Application reviews (2015/16)
- Data Security (2015/16)
- PSN (2015/16)
- Infrastructure (2014/15).

4.5.7 Other sources of authoritative guidance include the following:

- National Cyber Security Centre – 10 steps for monitoring to detect attacks.
- CIS Critical Security Controls for Effective Cyber Defence.

5 Conclusions

5.1 The audit identified three 'High' and three 'Medium' rated recommendations, giving, at this stage, a LIMITED level of assurance for the Council's compliance with the impending General Data Protection Regulations. It is recognised that the new Data Protection Officer post-holder should be in place now and some of the issues identified at the time of the audit may now have been, or are being, tackled and this will be reflected in the management responses to the findings.

5.2 The assurance bands are shown below:

Level of Assurance	Definition
Substantial Assurance	There is a sound system of control in place and compliance with the key controls.
Moderate Assurance	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

6 Management Action

6.1 The recommendations arising above are reproduced in the Action Plan for management attention.