Appendix 4

Audit Reports with Moderate or Low Level of Assurance issued Quarter 3 2019/20

Cloud Applications – 25 October 2019

1 Introduction

1.1 In accordance with the Audit Plan for 2019/20 an audit review of cloud applications was completed in September 2019. 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 This audit was undertaken to ensure that adequate controls are in place to protect the security, integrity and availability of data stored on Council cloud-based applications.

3 Scope and Objectives of the Audit

3.1 The audit was designed to assess and provide assurance on the following key areas:

- Information security guidelines on Cloud applications
- Access control including two factor authentication
- Proxy server protection to prevent access to insecure or unauthorised cloud applications
- External security testing
- Resilience and Disaster Recovery protection
- 3rd party Contracts including confidentiality and GDPR agreements.

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.

4 Findings

4.1 Recommendations from Previous Report

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

4.2 **Information security guidelines**

4.2.1 Key ICT policies and procedures relevant to the management and security of cloud-based applications were identified and obtained during the course of the audit. These were used in the process of reviewing the adequacy and completeness of the controls in place around cloud applications.

4.2.2 The policies identified as being of particular relevance in this review are the; 'Information Security and Conduct Policy', 'Privacy Impact Assessment Toolkit', and the 'Software Policy'.

4.2.3 Of the policies and procedures obtained and reviewed during the audit it was noted that the 'Privacy Impact Assessment Toolkit' document requires review and updating to reflect changes in the processes and procedures since the last update and to reference GDPR.

Risk

The privacy impact assessment process may be inconsistently performed.

Recommendation

The 'Privacy Impact Assessment Toolkit' document should be reviewed and updated.

4.2.4 It was also noted that the current version of the 'Software Policy' does not mention the privacy impact assessment process or reference the 'Privacy Impact Assessment Toolkit' document.

Risk

Privacy impact assessments may not be performed leading potential breaches of DPA and/or GDPR requirements.

Recommendation

The 'Software Policy' should be updated to reference the 'Privacy Impact Assessment Toolkit' process.

4.3 **Access control including two factor authentication**

4.3.1 Two cloud-based applications were selected in conjunction with management to be the basis for review as part of this audit. These were the ArtifaxEvent and Get Scheduled applications.

4.3.2 An understanding of the system management and access control arrangements in place for the applications tested was obtained through discussion with ICT and system owners and review of available process documentation.

4.3.3 User set up, change and removal processes were walked through and key application security controls including authentication controls and password settings were obtained and reviewed for each of the systems tested. This highlighted the issues detailed below.

4.3.4 It is good security practice to ensure complex passwords are in use and enforced by strong password security controls. A review of 'Get Scheduled' password parameters identified the system does not currently enforce strong password complexity requirements.

Risk

There may be unauthorised access to application data due to the use of weak passwords.

Recommendation

Management should liaise with the supplier to increase Get Scheduled password complexity requirements.

4.3.5 It was noted that the ArtifaxEvent application has the facility to implement two factor authentication but that this was not currently in use. It is recommended that management consider implementing this in order to provide improved security.

Risk

There may be unauthorised access to application data due to the use of weak passwords/ password sharing.

Recommendation

Management should investigate options around implementing two-factor authentication to the ArtifaxEvent application.

4.4 **External security testing**

4.4.1 An annual exercise of external penetration testing of the Council's infrastructure is undertaken as part of the annual IT Health Check (ITHC) exercise required as part of the PSN accreditation process. This is used to ensure the Council network is adequately protected against known vulnerabilities.

4.4.2 Additional ad hoc vulnerability scanning and penetration testing exercises are performed in conjunction with third party consultants on a risk basis, where deemed necessary throughout the year.

4.4.3 The two applications focused on as part of this audit are cloud-based services hosted by external suppliers, meaning the Council is reliant on the third party to secure the data appropriately.

4.4.4 A privacy impact assessment process is in place for use when implementing or making changes to systems, enabling management to gain some assurance around the security of data being held and processed. It was found during the work that this exercise had been completed for the Get Scheduled application but not ArtifaxEvent.

4.4.5 Although the risk is mitigated to some extent by the fact that the Council moved to a cloud-hosted service provided by the existing supplier that provided the previous version of the system, it is recommended that the privacy impact assessment be completed to ensure all privacy and security issues have been considered and documented.

Risk

Personal data may be held insecurely and/or breach DPA requirements.

Recommendation

The privacy impact assessment process should be completed retrospectively for the ArtifaxEvent system.

4.5 **Resilience and Disaster Recovery protection**

4.5.1 It was confirmed during testing that for both ArtifaxEvent and Get Scheduled backups of data and recovery arrangements are included as part of the service provided by the supplier. No recent outages or significant downtime was reported by management for either application.

4.6 **3rd party Contracts**

4.6.1 The contract and terms and conditions in place in relation to the Get Scheduled application were obtained and reviewed as part of the audit. It was found to have undergone review by the Council's procurement and information governance teams and to include the required references to GDPR obligations around data security.

4.6.2 It was not possible to obtain the ArtifaxEvent contract in the timescale required for this review. It is recommended that the privacy impact assessment recommended above (4.4.5) includes a review of the contract to ensure it meets Council requirements.

5 **Conclusions**

5.1 The audit did not highlight any urgent issues materially impacting the Council's ability to achieve its objectives. The audit did, however, identify four Medium rated and one Low rated issues which, if addressed, would improve the overall control environment.

Overall, the findings are considered to give MODERATE assurance around the management of cloud applications.

5.1 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.

Information Systems Policies – 25 October 2019

1 **Introduction**

1.1 In accordance with the Audit Plan for 2019/20 an audit review of the Council's information system policies was completed in September 2019. 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 This audit was undertaken to review the existence and adequacy of the Council's information systems policies.

3 **Scope and Objectives of the Audit**

3.1 The audit was designed to assess and provide assurance on the following key areas:

- Policy framework for data protection, records management, information security and data sharing
- Information security policy
- Policies are published on the Council's intranet
- All policies follow an agreed format and styling
- New and existing policies are subject to regular review
- Information systems technical build standards.

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.

4 Findings

4.1 Recommendations from Previous Report

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

4.2 Policy framework

4.2.1 An understanding of the policies in place for the management of information systems was obtained through discussion with ICT management during the audit. An information security and governance policy framework incorporating key elements including data protection, records management, information security and data sharing was found to be in place at the Council.

4.2.2 Key policies making up the framework were identified and obtained during the review. These were used in the process of reviewing the adequacy of the policies in in operation at the Council and key findings are detailed below.

4.3 Information security policy

4.3.1 The high level 'Information Security and Conduct Policy' describes the overall approach to information security and details a number of sub-policies that make up the framework. This policy, and sub-policies, documents the controls and processes in place to ensure that information is appropriately secured against issues arising that impact the confidentiality, integrity, and availability of Council data.

4.3.2 This policy was reviewed and found to document and define key information security roles and responsibilities, the Council's approach to maintaining the security and confidentiality of information, and includes references to all relevant sub-policies.

4.3.3 A sample of sub-policies was selected and reviewed for completeness and adequacy. This identified that the 'Information Security Incident Reporting' policy is in need of updating to reflect changes to requirements around the reporting of security incidents introduced as a result of GDPR. The policy currently states, for example, that there is "*no legal obligation in the Data Protection Act to report losses*" to the ICO, and makes no reference to the 72-hour timescale introduced as part of GDPR.

Risk

There may be a potential breach of GDPR requirements regarding incident reporting.

Recommendation

The 'Information Security Incident Reporting' policy should be

reviewed and updated.

4.4 **Information Governance Policies**

4.4.1 It was noted in discussion with management that an exercise to review and update information governance policies and procedures was ongoing at the time of audit and that work was required to substantially update policies covering data retention, data handling and classification of data in particular.

Risk

There may be ineffective information governance processes and controls in the absence of documented policies.

Recommendation

Ongoing work to update data retention, data handling and classification policies should be completed and updated policies should be made available to staff.

4.4.2 It was noted during testing that there has not historically been a process in place to ensure that data retention schedules are regularly reviewed and updated. As information asset owners have recently been assigned to all information assets it is recommended that an exercise to review retention schedules to sure they remain valid is undertaken and that this is repeated on an annual basis.

Risk

Data may be held longer than required and/or disposed of in breach of legal requirements.

Recommendation

Data retention schedules should be brought up to date and a regular review process should be introduced.

4.5 **Policies are published on the Council's intranet site**

4.5.1 Information system security and governance policies tested as part of this audit were found to be made available on the Council's intranet site.

4.5.2 Key information governance policies including the Information Governance Management Framework, Data Protection and Privacy Policy, Information and Access Rights, Records Management Policy, Information Security Incident Management Policy are also published on the external-facing Council website.

4.6 **Agreed format and styling**

4.6.1 Policies reviewed during the audit were found to follow a standard template,

with some minor exceptions. The policy template includes: a revision and version history section listing the dates of review and detail of any changes made; a section covering policy governance requirements including detailing the person(s) responsible for developing and implementing the policy and the person ultimately accountable; the required distribution of the policy; and any relevant references to other Council policies or legislation.

4.7 **Regular review of policies and procedures**

4.7.1 There is a Council requirement that all policies should be reviewed on an at-least annual basis. Testing was undertaken to determine the date of last review for key policies reviewed during the audit.

4.7.2 Testing identified that, in the majority of cases, policies are reviewed and updated frequently in accordance with Council policy and that the documents revision history is updated to reflect the changes made.

4.7.3 It was noted, however, that a number of key information governance polices are overdue for updating having last been reviewed on dates ranging from February – April 2018. It is understood from discussion with management that this is due to the significant amount of work and changes to policies and procedures required as a result of GDPR and that work on bringing these up-to-date is underway.

Risk

There may be an impact to systems / services in the event of incorrect procedures being followed in the absence of up-to-date policies.

Recommendation

All remaining policies should be reviewed and updated.

4.8 **Information systems technical build standards.**

4.8.1 The Council's approach to build standards is documented as part of the 'ICT Services System Lockdown Policy'.

4.8.2 The policy includes the requirement that a standard build process should be used for all Council desktop computers in order to minimise the risk of damage to the network due to the lack of security software, ensure a standard environment to aid software deployment, and help ensure software licensing compliance. This process is monitored by the use of a checklist each time a desktop or 'thin client' is built. A similar checklist was found to be in place for virtual servers.

4.9 **Record of processing activities**

4.9.1 GDPR requirements state that organisations must "*maintain a record of processing activities under its responsibility*" and define the minimum criteria that must be recorded in relation to the data held.

4.9.2 Testing identified that the Council is currently working on a comprehensive record of processing activities. Although a record of processing activity spreadsheet is currently in place for each Council department, it is noted that these are at varying degrees of completion, with some containing missing data.

4.9.3 While individual service areas have a responsibility to review and update this record on a regular basis, it is recommended that a regular oversight exercise be undertaken to ensure the record of processing activity is kept up to date. An exercise to audit a sample of departments from across the Council to review the completeness and accuracy of this data is also recommended.

Risk

There may be a breach of GDPR requirements regarding the need to demonstrate compliance.
Recommendation

An exercise to review the accuracy and completeness of the Council's record of processing activities should be undertaken on a regular basis to ensure the record is up to date. Management should also consider audits of individual departments to verify the accuracy of data in the record.

5 Conclusions

5.1 The audit did not highlight any urgent issues materially impacting the Council's ability to achieve its objectives. The audit did, however, identify five Medium rated issues which, if addressed, would improve the overall control environment.

As a result, the findings are considered to give MODERATE assurance around the management of information systems policies.

5.1 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.

Health and Safety Compliance of Council Buildings – 4 November 2019

1 Introduction

1.1 In accordance with the Audit Plan for 2019/20, 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.

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 audit had been included in the plan as a result of a specific request from management. This was largely as result of a review performed by the Head of Health & Community Protection (HHCP) of the various health and safety related compliance issues that the Council was responsible for.

2.2 The HHCP advised that an 'Asset Baseline' spreadsheet had been produced covering all of the different checks that should be performed but highlighted that it had been produced at a certain point in time which was prior to the restructure of the Assets section and the associated formation of the Compliance team.

2.3 During the course of the audit, it was established that an 'Assets Compliance and Delivery Group' had been formed which was to involve staff from the Assets section as well as those who were responsible for the management of different buildings operated by the Council. The inaugural meeting of this group (planned for mid-September) was due to discuss the terms of reference which was proposed to include the oversight of the areas included on the Asset Baseline spreadsheet.

3 Scope and Objectives of the Audit

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

3.2 The 'Asset Baseline' spreadsheet was the starting point in terms of the areas to be covered. However, due to the limited resources for the audit, not all areas identified could be reviewed. Therefore, in terms of scope, the following areas were covered:

- Electrical safety
- Gas safety

- Legionella
- Fire safety
- Lifts and lifting equipment
- 'Permits to work'
- 'Section 4 conditions'

3.3 The control objectives examined were:

- Council buildings are free from electrical safety risks
- Electrical equipment used by staff and visitors is safe to use
- Council buildings are free from gas safety risks
- Staff and visitors to Council buildings are free from the risk of exposure to Legionella bacteria
- Fire alarms will sound as appropriate
- Fire extinguishers will work if, as and when required
- Council buildings are free from fire safety risks
- All lifts and lifting equipment in place within Council buildings are safe to use
- The Council complies with COSHH regulations in regards to permit to work procedures
- The Council complies with Section 4 of the Health & Safety at Work Act 1974 with regards to the health and safety risks at premises leased to others.

3.4 The audit was only concerned with 'operational' corporate properties. Some, related, testing had recently been carried out on housing properties under the audit of Gas and Electrical Safety Checks.

3.5 Asbestos was also not included, as specific audits of Asbestos Management are undertaken, and other topics were also not to be covered where they are only related to individual specific assets.

3.6 The 'Section 4 Conditions' mainly apply to non-operational buildings. However, as these audits have recently been completed and this topic was not covered, it is being considered as part of this audit.

3.7 Whilst a number of building managers were spoken to as part of the audit, a specific review of their overall roles and responsibilities was not included within the scope. The HHCP advised that there is a general need for these roles and responsibilities to be clarified and communicated to all relevant staff and training is to be provided to them in due course.

4 Findings

4.1 Recommendations from Previous Report

4.1.1 This is the first audit of this topic, so this section is not relevant.

4.2 Electrical Safety

4.2.1 A contract is in place with Dodds Group (Midlands) Ltd (Dodds) for the Maintenance & Repair of Electrical Appliances & Installations. This covers

both domestic and corporate properties. The contract was reviewed under the recent audit of Gas & Electrical Safety Checks (for housing properties) so was not covered as part of this audit.

4.2.2 The M&E & Energy Officer (MEEO) advised that corporate properties are to be tested every three years. He suggested that there was no set programme, but the checks are easy to book in and would be done when it was noted that a building was due for a check with the checks being arranged with the relevant building managers.

4.2.3 Reports from the checks are scanned and held on the system with Active H being updated accordingly following the completion of the checks. The Data Coordinator (DC) provided an extract from the Active H system showing corporate properties that had various attributes, one of which was the EICR attribute.

4.2.4 An initial overview of the spreadsheet highlighted a number of properties for which the last cyclical (testing) date was either 1950 or 1955 so, before a sample of properties was chosen for testing, these were queried with the MEEO in order to ensure that the sample chosen for testing was relevant.

4.2.5 A list was then sent to Dodds of all the properties that the MEEO and the Compliance Team Leader (CTL) believed needed to be tested and Dodds provided the current status of those tests (i.e. whether they were required and in-date).

4.2.6 This list was compared to the Active H extract that had been provided initially and a number of gaps were noted. The MEEO suggested that these properties may not need EICRs and the attributes could therefore be disabled. However, this needs to be confirmed.

4.2.7 The Dodds list also identified a number of properties that were overdue for the EICR test. The CTL advised that Dodds were working through these to get them up to date. As a result, no testing of this aspect was undertaken.

4.2.8 However, sample testing was undertaken to ensure that documentation was held as appropriate with a sample taken from the confirmed tests as per the Dodds list. This testing proved generally satisfactory although three more instances were identified which no longer required the EICR attribute to be active.

4.2.9 One of these related to a property that was leased out so it was no longer up to the Council to undertake the tests and the other two were cases where the tests were either undertaken on individual properties within a larger property (e.g. lodges within a cemetery) or vice versa (i.e. the individual building 'element' is covered within a larger structure (e.g. toilets within a car park).

Risk

Council properties may not be safe from electrical safety risks.

Recommendation

A review should be undertaken of the properties with 'active' EICR attributes on Active H to ensure that this accurately reflects the properties for which EICR tests are required.

4.2.10 In terms of any remedial works required, the MEEO advised that Dodds would do the work although, if significant, further authorisation may be required. During testing, a number of notes were found to have been recorded on the certificates produced. The majority of these were recommended works (code C3) and this issue has been raised (as an advisory) in the recent Gas & Electrical Safety Checks audit report.

4.2.11 The MEEO advised that portable appliance testing (PAT) is undertaken by Dodds as part of the abovementioned contract. Whilst the contract does not specifically mention PAT, the MEEO advised that this is covered as part of the general works described in the corporate properties section of the specification.

4.2.12 The MEEO advised that there should be a programme for portable appliances to be tested every twelve months, with other equipment being covered every three years. However, he suggested that he was reliant on building managers flagging up when testing needed to be undertaken and there is no 'scheduled' programme for the testing.

Risk

Electrical appliances used in Council properties may be unsafe.

Recommendation

A schedule of PAT testing should be set for each relevant Council property.

4.2.13 The MEEO also advised that he thought Dodds would have a list of what had been tested, but there was no central inventory maintained. Part of the issue is due to new items being bought by individuals / teams and another issue is staff bringing in items of electrical equipment and the responsibilities for having them tested.

4.2.14 Building Managers spoken to confirmed that they did not generally maintain inventories of equipment that needed PAT testing, although the Technical & Facilities Manager (TFM) at the Royal Spa Centre advised that some technical equipment is (usually) tested by his own staff and a record of this is maintained.

Risk

Electrical appliances used in Council properties may be unsafe.
Recommendation

Inventories of electrical equipment that require PAT testing should be maintained for each relevant Council property.

4.3 **Gas Safety**

4.3.1 The extract from Active H (see 4.2.3 above) also included details of those properties where the Gas Safety attribute was active. This list included Jubilee House which had recently been switched to mains gas.

4.3.2 The MEEO advised that it is only boilers that are generally serviced, so there is no requirement to list all individual appliances.

4.3.3 A contract is in place with D&K Heating Services Ltd (D&K) for Gas Servicing and Maintenance of **Domestic** properties. The MEEO suggested that this had been varied to cover corporate properties as well. However, no evidence of this variation could be located at the time of the audit.

Risk

The Council may not have a contract in place for the undertaking of gas safety checks at operational Council properties.

Recommendation

The variation to the original contract should be confirmed with D&K.

4.3.4 Sample testing was undertaken to ensure that gas safety checks were being performed and documented as appropriate with the system being updated accordingly and any works identified as being required were undertaken as appropriate.

4.3.5 The only issue identified during the testing was that one certificate included a note about potential works required. However, the certificate stated 'see PDA' as opposed to detailing the issue encountered.

4.3.6 The MEEO advised that a supporting email may have been sent, but this would not have been saved alongside the certificate.

Advisory

Contractors should be advised that any issues identified should be appropriately recorded on the certificates provided to the Council.

4.4 **Legionella**

4.4.1 A contract is in place with HSL (formerly Hertel Solutions Ltd) for Legionella and Water-Quality Management. The contract register suggested that no copy of the contract was held in the Document Store or in electronic format. However, the MEEO advised that copies of the document had recently been located and a copy was provided.

4.4.2 The extract from Active H (see 4.2.3 above) also included details of those

properties where the Legionella Management attribute was active. The MEEO advised that risk assessments will have been performed for each relevant building.

4.4.3 Sample testing was undertaken to ensure that the risk assessments are in place, monthly testing is being undertaken by the contractor and systems are being disinfected where appropriate. This proved satisfactory.

4.4.4 Testing was also to be undertaken on the weekly flushes that are meant to be undertaken at each building. However, the records are maintained at each site and were not readily available without performing individual site visits.

4.4.5 Copies were requested when meetings were held with building managers, but only one of three was returned during the timescales of the audit.

Advisory

The Assets Compliance & Delivery Group should reiterate the need for weekly flush records to be maintained by relevant building managers.

4.5 **Fire Safety**

4.5.1 The MEEO advised that fire alarms are tested on a weekly basis by Fire Safe Services (see below). A test sheet is run through and a log is sent to building managers although no central record is maintained.

4.5.2 The MEEO advised that he is (currently) having issues getting emails from the contractor relating to the tests at other sites. He used to get the emails relating to tests at Riverside House but these are currently not being received due to IT issues. However, he advised that he is confident that the tests are undertaken at Riverside House as he can hear them being tested.

4.5.3 In terms of Oakley Woods Crematorium, the Bereavement Services Development Manager (BSDM) advised that there were issues with their alarms in that the alarm for one building cannot be heard in the other and vice versa. However, she advised that this is being looked into. Other building managers spoken to confirmed that tests were operating satisfactorily.

4.5.4 A contract is in place with Fire Safe Services for the Service and Maintenance of Corporate Fire Alarms. Similar to the Legionella contract, the contract register suggested that no copy of the contract was held in the Document Store or in electronic format. However, the MEEO advised that copies of the document had recently been located and a copy was provided. He also provided a copy of the list of 'assets' that Fire Safe Services cover under the contract.

4.5.5 The MEEO advised that the systems are serviced on a quarterly basis, with different aspects covered each quarter against a plan / routine ensuring all aspects are covered over course of the year. This 'plan' is detailed on copies

of the servicing worksheets provide.

4.5.6 Sample testing was undertaken to ensure that fire alarm systems are being maintained appropriately with documentation being held to support the tests undertaken. This test proved generally satisfactory although the latest service for one sampled building (Victoria Park Cricket Pavilion) was overdue at the time of the audit.

Advisory

The quarterly service of the fire alarm at Victoria Park Cricket Pavilion needs to be followed up with the contractor to establish why it had not been performed.

4.5.7 A contract is in place with Baydale Control Systems Ltd for the 'servicing, testing, certification, reactive maintenance and ad-hoc installation of Fire Fighting Equipment'. This was a variation to their existing contract that covers Door Entry Systems, CCTV, Security Doors and Fire Alarm Systems Maintenance and Upgrade.

4.5.8 In terms of 'programming' the intention is that all equipment is checked every twelve months and the contractors know when they are due to be checked. These checks are booked in with the individual building managers with the contractors having contact details. However, the MEEO suggested that some equipment has been missed from the programmed checks.

4.5.9 This was corroborated by BSDM who advised that their visit had not been booked on an appropriate date, so some equipment had been missed as a service was ongoing.

4.5.10 Sample testing was undertaken to ensure that inventories of relevant fire fighting equipment are maintained and that maintenance had been undertaken for each item held with replacement equipment being provided where necessary.

4.5.11 Inventories were found to be in place for each sampled building and maintenance records were provided for each one. In two instances some of the extinguishers were found to be in need of replacement and these replacements had subsequently been ordered.

4.5.12 The inventories do not go into detail as to serial numbers etc. so replacements do not need to be reflected on the inventory (assuming like-for- like replacements). However, a number of handwritten amendments were found to be detailed on two maintenance records and these had not been reflected on the inventories held. The MEEO advised that the updating of inventories was a known issue and responsibility needed to be assigned to this task.

Risk

Fire fighting equipment may be omitted during programmed maintenance and testing and may not work if required.

Recommendation

Inventories of fire fighting equipment should be kept up to date to ensure that contractors are aware of what neds to be tested.

4.5.13 The Building Manager & H&S Coordinator (BMHSC) advised that Fire Risk Assessments are undertaken for all relevant Council buildings on a regular basis by staff from Building Control. The assessments are then loaded onto AssessNet.

4.5.14 The Principal Building Consultant (PBC) advised that, due to staffing levels, the frequency of assessments has been assessed to ensure that the buildings with the higher risk are covered more frequently.

4.5.15 A report was produced from the system that showed all of the assessments that had been performed and this confirmed that the review dates (where stated) were all in the future. One assessment was due in the near future, but the PBC highlighted that that type of building (toilet blocks) was very low risk so this was not a high priority.

4.5.16 One assessment did not include any review details (re Saltisford Gardens Community Centre). However, the BMHSC confirmed that the record was covered under another assessment which was for the same building.

4.5.17 The BMHSC advised that AssessNet also includes a record of all the 'tasks' that are associated with the fire risk assessments (i.e. issues that need to be addressed). These are assigned to staff at the individual buildings to resolve and sample 'tasks' were covered during the meetings with building managers.

4.5.18 The tasks shown as being relevant to the Arts buildings and the Enterprise buildings were shown as being complete. However, a number of tasks appeared to be outstanding against Bereavement Services buildings.

4.5.19 The BSDM raised a number of issues with the assessments, including tasks appearing to be superseded by subsequent actions and system access allowing relevant staff to update the system as required. The Business Support & Development Manager advised that this was now being addressed following meetings with the BSDM, the BMHSC and Building Control staff.

4.6 **Lifts & Lifting Equipment**

4.6.1 A contract is in place with Stannah Lift Services Ltd for the 'provision of lift service and maintenance'. This just covers the items detailed in the spreadsheet.

4.6.2 In terms of lifting equipment, the BSDM advised that the equipment is maintained under the cremator plant equipment contract at Oakley Woods and the TFM advised that the equipment at the Royal Spa Centre had previously been maintained under warranty by the company that had

provided the system. However, it is due to be undertaken by another contractor this year although this had not yet been timetabled so no formal agreement was in place.

4.6.3 Sample testing was undertaken to ensure that lift servicing and maintenance was being performed as required with documentation being provided. The test proved satisfactory.

4.6.4 The MEEO advised that any remedial works picked up as part of the servicing are covered by the contract in place and, whilst not specifically identified upon review of the test documentation reviewed, it was clear that work was being undertaken as required through direct observation at Riverside House.

4.7 **Permits to Work**

4.7.1 The BMHSC advised that there are three main areas where permit to work procedures are required at the Council, i.e. working at height, 'hot work' and working in confined spaces. These issues would be picked up as part of the normal risks assessment process and via the method statements provided by the contractors.

4.7.2 A sample RAMS (Risk Assessment Method Statement) document was provided by the MEEO for Lightning Protection works and this makes specific reference to the requirement for permits within the risk assessment.

4.7.3 The current permits to work are recorded on AssessNet. However, the BMHSC highlighted that older documents had been 'lost' following a system upgrade, so there were only a few recorded on the system with the majority relating to the lightning protection works. The system also includes the sign-off declarations from relevant parties.

4.7.4 The BMHSC also highlighted that some of the permits to work shown on AssessNet are noted as being 'handed back'. In these instances, the permits cannot be used again so, if the same / similar job needs to be undertaken, a new permit will be required.

4.7.5 The MEEO advised that he is generally reliant on contractors to flag that permits are required and that it was up to individual building managers and contract managers to identify risks and, therefore, some works that require permits may be missed. In general, he felt that there was an education need and this was echoed by the building managers spoken to.

Risk

Permits to work may not be in place where appropriate.

Recommendation

Training on the need for Permits to Work should be provided to relevant staff, including individual building managers as

appropriate.

4.8 **Section 4 Conditions**

4.8.1 Section 4 of the Health and Safety at Work Act 1974 places a duty on those in control of premises, which are non-domestic and used as a place of work, to ensure that they do not endanger those who work within them. Where the Council leases a building to a tenant, the Council still has responsibilities to ensure that the buildings are being appropriately maintained (either themselves or by the tenant depending on the terms of the lease).

4.8.2 The Estate Management Surveyor advised that checks to ensure that the conditions are being met are not currently being performed and that they haven't been undertaken for a number of years due to varying factors such as staffing and responsibility changes. However, he advised that the need for compliance reviews has been recognised and a recruitment process is currently underway for a number of new Building Surveyors.

4.8.3 The Technical Manager advised that interviews were to be undertaken during the course of the audit for two fixed term appointments and that an advert was also out for other posts; it is hoped that, once these posts have been appointed to and a full staffing resource is available, visits will then be reinstated, with annual visits in the first instance.

4.8.4 The Business Manager (Enterprise) advised that the leases in place for the Court Street Creative Arches included reference to health and safety and that her staff are going through the process of asking tenants to provide (documentary) evidence to confirm that health and safety conditions were being met.

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 Health & Safety Compliance of Council Buildings 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.

5.3 A number of issues were, however, identified:

- It is unclear whether the EICR attribute details on Active H are accurate.

- There are no PAT testing schedules for Council buildings.
- There are no inventories for equipment that requires PAT testing.
- The contract variation relating to the inclusion of corporate properties in the 'gas maintenance' contract could not be located.
- Some inventories of fire fighting equipment were not up to date.
- Staff require training on when Permits to Work are required.

5.4 Further 'issues' were also identified where advisory notes have been reported. In these instances, no formal recommendations are thought to be warranted as there is no risk if the actions are not taken. If the changes are made, however, the existing control framework will be enhanced:

- One gas safety record included reference to works required being recorded on the PDA. This information should be on the actual record provided.
- Weekly flush records that were requested were not all provided during the timescales for the audit so these should be followed up by the new Assets Compliance & Delivery Group.
- The latest fire alarm service for Victoria Park Cricket Pavilion needs to be followed up with the contractor.

Catering Concessions – 19 December 2019

1 **Introduction**

1.1 In accordance with the Audit Plan for 2019/20, an examination of the above subject area has been completed recently and this report is intended to present the findings and conclusions for information and action where appropriate.

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

2 **Background**

2.1 Catering is provided at a number of Council-owned premises, the operations in most of these being run by external parties under lease agreements generating fixed rental income to the Council. Catering at the Council's sports and leisure venues are now subsumed within the respective outsourced management contracts.

2.2 This leaves only two sites where the Council has maintained a measure of direct commercial control through concession contracts – the Jephson Gardens 'Restaurant' in the Park' (also known as the 'Glasshouse' by which it will be referred to from here onwards) and the Royal Pump Rooms (public

Café and events in the Assembly Rooms/Annexe).

2.3 At the time of writing, the Royal Pump Rooms Café has ceased operating pending new arrangements expected to be lease-based. This leaves the Glasshouse as the sole remaining Council catering premises operating as a concession for the foreseeable future.

2.4 The concessions were executed under a single three-year contract in January 2019 with a preferred supplier nominated by the Regeneration Partner for the Creative Quarter. Arguably this makes it a sub-contract with the Regeneration Partner as main contractor, and has been referred to as such in relevant Executive reports. The proposals leading to the final concession contract had been approved by the Executive in May 2018 subject to negotiation on further details under delegated powers.

2.5 Originally for both premises, the concessions cover day-to-day operations and special events. The provisions governing recharges for premises and equipment service, along with the criteria for determining concession charges remain unchanged from the previous contract with Kudos.

2.6 Recent years' budgets indicate the Council's expectations for income generation to be around £75,000 per annum made up as follows:

	Amount (£)
Glasshouse – service charges	12,000
Glasshouse – concession charges	43,000
Pump Rooms Café - service charges	12,000
Pump Rooms Café - concession charges	8,000
	75,000

2.7 The closure of the Royal Pump Rooms Café was an inevitable consequence of an agreed scheme (approved by the Executive in October) to detach both the Café and Assembly Rooms/Annex event operations from the concession contract. This has had the effect of eliminating the involvement of the Creative Quarter Partnership in catering solutions for this site in the foreseeable future.

2.8 At the time of this report, two key initiatives are being progressed:

- marketing of Royal Pump Rooms Café availability for lease – vetting of expressions of interest are in progress;
- recruitment of an events officer to handle Royal Pump Rooms events subject to approval by Employment Committee.

3 Scope and Objectives of the Audit

3.1 The audit examination was undertaken for the purpose of reporting a level of assurance on the adequacy of controls for managing catering concessions operating at Council premises to ensure the realisation of relevant business objectives and compliance with the agreed conditions.

3.2 The examination was programmed based on a light-touch version of the standard Contract Management Audit Programme to evaluate in overview the structures and processes for managing the 'client' side of concessions

currently in place. In view of the aforementioned developments, a limited evidential review of the background to the original proposals in the context of 'provider' business strategy and planning was introduced into the scope.

3.3 In all, the areas considered in the examination were:

- business strategy and planning
- award of concession
- service provision and monitoring
- contract amendments and variations
- financial administration
- contingency planning and risk assessment.

3.4 The findings are based on discussions with David Guilding (Arts Manager) and examination of available public and internal Council documentation and records.

4 Findings

4.1 Recommendations from previous report

4.1.1 Both recommendations from the audit reported in March 2017 were made in the context of the former concession contract with Kudos and are therefore disregarded for the purpose of this examination.

4.2 Business Strategy and Planning

4.2.1 As the business strategy and planning elements were handled directly by the Regeneration Partner jointly with their nominated supplier, source information from which to evaluate the process was not available without direct approach to the external parties. This was not seen to be justified within the scope and resource for the audit.

4.2.2 The bulk of the evidence available to gain any picture here is contained in the submission to the Executive in May 2018, along with its attached appendices. These make references to business planning processes by the Regeneration Partner and the nominated supplier which indicate a sound basis behind the revenue projections offered.

4.2.3. By way of comment, however, comparison with actual revenue history indicated by concession outturn over a five-year period gave the impression that the projections offered were inordinately ambitious at best (even in the context of circumstances at the time of the submission). This observation is not suggested as the sole factor behind the financial shortfalls under the concession, as it is recognised that other unforeseen factors have manifested themselves.

4.3 Concession Award

4.3.1 The process leading to the award of the concession was bound up in the pre-existing Collaboration Agreement for the Creative Quarter. The Council is a direct signatory to the Deed of Agreement for the

concession along with the Regeneration Partner and the supplier.

4.3.2 The Agreement comes across as properly executed with appropriate specifications and key performance indicators. A formal, sealed original Agreement is held in the Document Store.

4.4 **Service Provision and Monitoring**

4.4.1 The aims and objectives of the concessions have become bound up within those of the wider Creative Quarter project.

4.4.2 The subsequent detachment of the Royal Pump Rooms with new management and lease arrangements does not appear to have impacted on the aims and objectives for that premises in relation to Fit for the Future and supporting strategies.

4.4.3 The key terms and specifications show as essentially unchanged from the previous contract. Evidence trails show that contract management arrangements were in the process of being established from the outset with attention starting to be given to performance outturn with the aid of customer feedback information.

4.4.4 However, the financial shortfalls began to overshadow all other considerations only a few months into the contract and the ongoing management processes have to be seen as in abeyance at the time of this report.

4.5 **Contract Amendments and Variations**

4.5.1 The detachment of the Royal Pump Rooms from the concession is well documented and warrants no further comment here.

4.6 **Financial Administration**

4.6.1 No meaningful process review of this area was possible with the relevant budgets based on already-outdated projections and an effective moratorium on income collection still in place at the time of the audit.

4.6.2 To date, only rates and some utility recharges under the current contract are in evidence and, even then, only up to June 2019. No concession charges have been raised to date under the current contract, nor the initial deposit required under the contract terms.

4.6.3 In addition, settlement of charges under the former contract totalling around £44,000 is still being pursued with the involvement of County Legal Services. It was advised that repair cost recharges included in the amount are in dispute and attempts at resolution are still ongoing at the time of this report.

4.6.4 Settlement of outstanding charges under the current contract is subject to a payment plan which is in the process of being agreed with the

supplier at the time of this report.

4.7 **Contingency Planning and Risk Management**

4.7.1 This has not been seen as an area where formal contingency plans can add impact mitigation value to existing monitoring processes. It is recognised that these processes have themselves proved successful in averting a complete break-down of operations under the concessions by facilitating agreement on a viable alternative.

4.7.2 Proof of up-to-date supplier's insurance has been reviewed and found to be in accordance with the contract terms.

5 **Conclusions**

5.1 It is difficult to give a single assurance opinion in respect of the audit as the circumstances noted in the report do not fit conveniently the prescribed assurance definitions. In particular, the issues arising are not, in the main, controls-based but perhaps more to do with judgements and events. In spite of this, Internal Audit is bound professionally to issue an assurance opinion. In arriving at an appropriate level of assurance, the following is being taken into account: On the one hand, there are concerns in respect of the closure of facilities and the reputational damage that is causing. Other concerns include factors such as the over-estimate of income projections and the legal situation the Council is now facing. On the other hand, much comfort can be gained from routine contract monitoring arrangements that identified the issues promptly so that a compromise solution could be worked out for the concessions in future. The legal situation also provides some reassurance in that attempts are being made to mitigate the losses.

5.2 With the requirement to issue an assurance opinion it would seem that a MODERATE level of assurance is suitable, reflecting an appropriate compromise between the areas of concern and the causes for comfort.