LICENSING, AUDIT AND GENERAL PURPOSES COMMITTEE
26 NOVEMBER 2018 **AUDIT MANAGER**
REPORT NO. AUD1805

INTERNAL AUDIT – AUDIT UPDATE

SUMMARY:
This report describes the work carried out by Internal Audit for quarter 2 and the proposed work to be delivered for quarter 3 and 4.

RECOMMENDATION:
Members are requested to:

i. Note the audit work carried out in quarter 2.
ii. Note the update to the expected deliverables for quarter 3.
iii. Endorse the expected deliverables for quarter 4

1 INTRODUCTION

1.1 This report is to provide Members with:

- An overview of the work completed by Internal Audit to date for quarter 2.
- An update of the progress made and any changes required for the expected deliverables for quarter 2 and 3, as approved by the Committee on the 30th July 2018.
- A schedule of work expected to be delivered in quarter 4.

2 RESOURCES

2.1 The Audit Manager has now returned from Maternity Leave full time. Additional contractor resources are still being provided by Wokingham Borough Council to enable the delivery of the Internal Audit Plan.

2.2 The resources within the Audit team are due to be reviewed by the end of the financial year.

3 AUDIT WORK – Q2 18/19

3.1 The following audit work has been carried out within quarter 2:

Work	Status
Audit findings – Appendix A of this report	
Purchase Ledger (carried forward from 2017/18)	This audit was carried out by the contract auditors. It was carried forward from 17/18. A ***limited assurance*** opinion has been given to this area. Findings are detailed within Appendix A.

GDPR	This audit was carried out by the contract auditors as per the schedule of work for quarter 2. A ***reasonable assurance*** opinion has been given to this area. Findings are detailed within Appendix A.
Cyber Security Follow up	A follow up was carried out on the recommendations made from the Cyber Security audit carried out in 2017/18. The findings from the follow up has made no change to the assurance opinion within this area, which remains as ***reasonable assurance***. Findings are detailed within Appendix A.
Separate reports to this November Committee	
Incident Management policy	A draft Incident Management policy has been developed in line with the requirements for GDPR. Being present to the Committee at this meeting as a separate agenda item.
Audit Charter	A draft Audit charter has been produced and is being present to the Committee at this meeting as a separate agenda item.
Items for the January Committee	
IT access controls	This audit has been carried out by the contract auditors. The testing has been completed and the draft report is currently being prepared. The findings will be communicated to the Committee at the meeting in January 2019
Waste contract	This audit has been carried out by the contract auditors. The testing has been completed and the draft report is currently being prepared. The findings will be communicated to the Committee at the meeting in January 2019
Weekly refuse and recycling contract	This audit has been carried out by the contract auditors. The testing has been completed and the draft report is currently being prepared. The findings will be communicated to the Committee at the meeting in January 2019
Parking Machine Income follow up	A follow up on the recommendations made within the Parking Machine Income audit carried out in 2016/17 is being carried out. The findings of this follow up will be communicated to the Committee at the meeting in January 2019.
Portable IT Equipment follow up	A follow up on the recommendations made within the Parking Machine Income audit carried out in 2017/18 is being carried out. The findings of this follow up will be communicated

	to the Committee at the meeting in January 2019.
Transparency code follow up	A follow up on the recommendations made within the Parking Machine Income audit carried out in 2017/18 is being carried out. The findings of this follow up will be communicated to the Committee at the meeting in January 2019.
Depot (carried forward from 2017/18)	This audit has been carried out by the contract auditors. The testing has been completed and the draft report is currently being prepared. The findings will be communicated to the Committee at the meeting in January 2019
Awaiting information	
Contaminated water review	This review has been completed but the report has yet to be issued, as it will be done in conjunction with the Contaminated soil review.
Contaminated soil review	Currently waiting on information to be provided by the contractors.

3.2 *Other deliverables:*
Work has also been carried out in order to establish the current demands on the Corporate Investigations Officers, who now come under Internal Audit, so that a work programme can be established for 2019/20 financial year and quarterly updates on their work reported to this Committee.

4 UPDATE TO AUDIT WORK FOR Q3

4.1 At the meeting on the 29th January 2018. It was agreed that if any changes were required to the agreed deliverables for the quarter, in order to meet changing needs of the organisations, then this would be communicated to the committee along with the reason for the change.

4.2 The following changes will be made to quarter 3 work previously planned within the audit update provided to the Committee in July 2018.

- Risk Management audit – This will now be carried out within quarter 4. This is to allow the new corporate risk register to be implemented within the organisation.
- Contract letting and tendering follow up – This was due to be carried out within quarter 2 but will now be carried out in quarter 3, due to resource availability.
- Corporate governance audit – This was due to be carried out within quarter 2 but will now be carried out in quarter 3 due to resource availability.

5 EXPECTED DELIVERABLES FOR Q3 AND Q4

5.1 The work expected to be delivered in quarter 3 and 4 is detailed within the table below. As with the previous quarter, these audits can be subject to change due to the changing needs of the organisation or resource availability. An update will be provided at the January meeting.

Service	Audit/ follow up/descriptor	Expected
Finance	Contract Management - *A review of how contracts are monitored within the Council to ensure they are delivering the outcomes we require.*	Q3
CLT	Corporate Governance - *Overview of corporate governance arrangements within the Council against CIPFA/SOLACE guidance.*	Q3
Finance	Benefits - *Key financial system review of the benefits system/process*	Q3
Finance	Recovery - *Key financial system review of the debt recovery system/process*	Q3
Finance	Sales Ledger - *Key financial system review of the sales ledger system/process*	Q3
Legal	Purchase of property follow up - *A follow up on the recommendations made within the audit carried out in 2017*	Q3
Finance	Card payments follow up - *A follow up on the recommendations made within the audit carried out in 2017*	Q3
Finance	Contract Letting & Tendering follow up - *A follow up on the recommendations made within the audit carried out in 2017*	Q3
Planning	Planning Applications - *A review of adherence to statutory requirements and processes for planning applications*	Q4
Housing	Disabled Facilities Grant - *A review of processes for granting DFGs and process for the rotation of suppliers.*	Q4
Finance	Capital Programme Management - *A review of the arrangements in place to manage the capital programme and the projects included.*	Q4

CLT	Risk Management - *A review of the risk management process and system in place. This is an area that was highlighted within the Annual Governance Statement and by External Audit as having deficiencies.*	Q4

AUTHOR: Nikki Hughes, Audit Manager
01252 398810
nikki.hughes@rushmoor.gov.uk

HEAD OF SERVICE: Peter Timmins, Interim Executive Head of Financial Services

References: *Internal Audit – Audit Plan* report, presented to the Committee on the 29th January 2018
https://democracy.rushmoor.gov.uk/ieListDocuments.aspx?CId=166&MId=459&Ver=4

Internal Audit – Audit update report, presented to the Committee on the 30th July 2018

https://democracy.rushmoor.gov.uk/ieListDocuments.aspx?CId=166&MId=553&Ver=4

Audit Title 1	**Purchase Ledger**		
Year of Audit	2017/18		
Assurance given	**Limited** – *Minimal controls designed to achieve the system/function/process objectives, are in place. Significant improvements are required if key controls are to be established.*		
Overview of area	The Purchase Ledger function is in place to enable accurate and timely payment for bona fide goods and services received by the Council. There are 3 potential types of payments for processing: proformas (non-invoice), IAS (Invoice Approval System/ non-purchase order) invoices and purchase order invoices.		
Priority	**Key findings**	**Management response and agreed action**	**Action by who and when**
High	There is currently no requirement, or system control, to incorporate separation of duties within purchase ledger transactions. The same person can requisition, GRN, and authorise payment. In some cases, this person will also be responsible for budget monitoring as the budget holder. This same person can also have suppliers set up on the system without authorisation from another member of staff, or verification of the suppliers' validity. ***Risk**: Without separation of duties or supplier set up controls, the Council is at risk of fraud and the processing of invalid payments to invalid suppliers.*	This is a risk that has previously been accepted by the management of the organisation. It is a balance between risk and efficiency. Complete separation of duties would increase the time taken to purchase and pay for goods. Any change would need to be supported by management. A detailed discussion at CLT would be required to agree a way forward.	Action by CLT – The report was taken to CLT in August 2018 for discussion.
High	The Purchase Ledger team do not carry out validity checks on new suppliers and there is no requirement for the set-up of a new supplier to be agreed by more than one member of staff. (It is possible that the Contracts team perform checks on some suppliers; the Purchase Ledger team may wish to co-ordinate with the Contracts team to ensure this control is in place without duplicating effort.	Independent verification of changes to bank details and audit of this work by finance team feels sufficient. A new supplier form could be designed with some necessary checks to be completed - wider discussion required on what checks to carry out and who should be responsible for this.	Action by CLT – The report was taken to CLT in August 2018 for discussion.

	Risk: *Without separation of duties or supplier set up controls, the Council is at risk of fraud and the processing of invalid payments to invalid suppliers.*		
Medium	For IAS invoice transactions, spend is not committed to the Integra 2 system until the invoice is received. ***Risk:*** *If spend commitment is not included in the corporate financial management system, reports from the system used to inform decision making may be inaccurate****.***	Cannot raise commitments on the IAS system – only way to do this is to only use the purchase ordering system.	N/A
Medium	For IAS transactions, there is no requirement to confirm that goods/services have been received (GRN completed) before payment. ***Risk:*** *This increases the risk of payment being made for goods/services that have not been received and for duplicate payments.*	The system does not allow for GRN of IAS invoices – again the only resolution is to move wholly to POs – not always practical.	N/A
Medium	When blank cheques are taken from the safe, the first and last cheque number is recorded. During the cheque run for purchase ledger, one person removes the cheques from the safe. ***Risk:*** *It is possible for this person to remove cheques from the middle of the pile without being noticed – this would potentially not be picked up for some time as a number of people can access the safe; it would not be easy to identify when the cheques were removed or by whom.*	The Payments and Insurance Manager has advised staff that two officers should be present for the cheque payment run.	Payments and Insurance Manager – February 2018
Low	IAS invoices do not show a purchase order valid to the Integra 2 system (different system orders such as those raised using the CONFIRM system are not compatible with Integra 2) and some do not give a contact at RBC.	Again, could insist on use of POs – would need to be a management decision. Reminding managers/suppliers to ensure a contact name is always provided	Action by CLT – The report was taken to CLT in August 2018 for discussion.

	***Risk**: If experienced staff with local knowledge are lost, there is a risk that allocating an invoice could become labour intensive and inefficient.*	seems a proportionate response.	
Low	High payments checks are set at a £15k limit for historical reasons that no longer apply; the limit for countersigning cheques is £25k. ***Risk:** Checks may be being carried out unnecessarily.*	Report requires changing – Finance Manager can follow this up with internal system report expert	Finance Manager – August 2018
Low	Payment run supporting paperwork is held in hard copy only. ***Risk**: Hard copy files increase the use of paper/ storage and are less accessible than electronic storage methods.*	Explore ways of holding data electronically Explore ways of reducing paper storage eg retaining first and last page of documents that record no anomalies and signing	Finance Manager – October 2018
Low	Purchase Ledger procedural guidance is not currently version controlled. ***Risk:** It is not clear whether guidance is up to date.*	The Payments and Insurance Manager has added a review date to procedural guidance.	Payments and Insurance Manager – February 2018
Low	In sample testing, 1 out of a sample of 25 tested did not comply with HMRC requirements for VAT claims as the invoice did not show and RBC address. ***Risk:** The Council may not be able to reclaim VAT*	The Payments and Insurance Manager has reminded the relevant member of staff of HMRC requirements and the need for an RBC address on invoices.	Payments and Insurance Manager – February 2018

Priority key for way forwards	
High priority	A fundamental weakness in the system/area that puts the Authority at risk. To be addressed as a matter of urgency.
Medium priority	A moderate weakness within the system/area that leaves the system/area open to risk.
Low priority	A minor weakness in the system/area or a desirable improvement to the system/area.

Audit Title 2	GDPR		
Year of Audit	2018/19		
Assurance given	**Reasonable** – *Basic controls designed to achieve the system/function/process objectives, are in place. Improvements are required if key controls are to be established.*		
Overview of area	This is the first audit review of information processing systems, policies and processes since the Data Protection Act 2018 and General Data Protection Regulation (GDPR) came into force on 25th May 2018. The project to implement measures to meet the requirements of GDPR has been led by the Legal Services Manager and Corporate Projects Manager. However, with the recent departure of the Corporate Projects Manager, the Legal Services Manager has continued the hard work to bring systems and processes up to the required standards with the assistance of a new interim Project Manager. The impact of GDPR and the potential risks faced by local authorities over non-compliance should not be underestimated. The headline being fines of up to twenty million Euros or four percent of annual turnover (whichever is highest) for non-compliance. However, significant benefits can be drawn from the changes, such as fostering the public's trust in how the council obtains, stores and uses personal information, and how it co-operates with the public and regulators following data breaches.		
Priority	**Key findings**	**Management response and agreed action**	**Action by who and when**
High	**Project Management** The role and timescale of the interim GDPR Project Manager is not fully defined. The Project Manager role is essential to driving forward work, such as identifying how services manage customer consent to processing data, information archiving, staff and member training, information asset registers, Registers of Processing Activities, data sharing agreements, co-ordinating service representatives, and contracts compliance.	Following the departure of the Project Manager, interim project support along with a subject matter expert in data protection were allocated for an interim period, until the Corporate Legal Manager (DPO) commences. At that stage, an assessment of the project status and resources to move the work forward will be undertaken.	Ian Harrison, Corporate Director – January 2019

	***Risk**: On-going progress of the GDPR Project Plan may not be managed and realised.*	Additionally, to strengthen the governance the Corporate Director, Heads of Finance and IT & Facilities are meeting monthly (Governance Group) to provide programme oversight. At the same time, further links were made to the council's Risk Management Group.	
Medium	**Training** Only senior/middle management have undertaken formal GDPR training with it still outstanding for the Chief Executive, officers and Members. Member briefings were undertaken. ***Risk**: In the event of a serious breach, it could not be proven that the council had taken all reasonable steps to ensure good awareness for all officers and Members.*	Training for Members is booked in for November 2018 and January 2019. A decision has been made to use the existing e-learning package and the Project Team are currently identifying relevant training content to be set up.	Project team/ Legal Services Manager – January 2019
Medium	**Training** Resource to create, test and deliver e-learning training for officers is insufficient. ***Risk**: The provision of E-learning training will be further delayed.*	A decision has been made to use the existing e-learning package and the Project Team are currently identifying relevant training content to be set up.	Project team/ Legal Services Manager – January 2019
Medium	**Project Reporting** a) Previously, 'highlight' reports have been sent to CLT for their consideration of issues, risks and other actions. GDPR has not been formally reported to CLT of late.	a) Following the departure of the Project Manager, interim project support along with a subject matter expert in data protection were allocated for an interim period, until the Corporate Legal Manager (DPO)	Ian Harrison, Corporate Director, Head of IT & Facilities and Corporate Legal Manager – January 2019

	b) Meetings with service representatives were an effective means of communicating risks, information and project progress, but have reduced in frequency and should therefore be continued regularly. ***Risk**: Data security risks and project slippage could manifest if issues are not regularly communicated to CLT and service representatives.*	commences. Additionally, to strengthen the governance the Corporate Director, Heads of Finance and IT & Facilities are meeting monthly (Governance Group) to provide programme oversight. At the same time, further links were made to the council's Risk Management Group. b) Communication is to be placed on the StaffHub in early November 2018, updating officers on GDPR and the next steps, including the role of service reps.	
Medium	**E-mail Classification** For e-mails issued by all management, officers and Members, there is no standard Document Protective Marking system prompt to classify the content, e.g. Unclassified, Official, Official-Sensitive. ***Risk**: E-mail content and attachments may be sent without the appropriate classification of importance and sensitivity of data.*	The IT solution is in place and could be implemented, however, prior to implementing, the Project Team would like to clarify with the ICO and seek a view from the newly appointed Corporate Legal Manager (DPO). For existing specific users who are involved in sensitive data transmissions, GCSX accounts are already used.	Corporate Legal Manager and IT Technical Services Manager – January 2019
Low	**Risk Management** There is a risk register for GDPR on SharePoint to track the project's risks, but it is incomplete. Each risk has an assigned 'likelihood', 'impact' and composite 'risk value'. All risks, except 7 and 8, have an assigned 'action' (Treat, Tolerate,	Agreed and will be updated.	IT Project Manager – action immediately

	Terminate or Transfer). ***Risk**: Risks relating to GDPR may not be managed effectively.*		
Medium	**Mapping of Information** Information Asset Registers have been created to capture the information held by each service and the measures in place to keep it secure. Standard (and highest risk) data has been captured, but work remains for Special Category data and overall completeness. Article 30 of GDPR requires a Register of Processing Activities (RoPA) to be completed also. This has yet to be done, but the mandatory fields of the RoPA could be incorporated in to the Information Asset Register template. ***Risk**: The GDPR regulations are not fully complied with.*	Service reps are to continue to classify their Special Category data and their lawful basis for holding this data. Arising from these classifications, the ROPA will be created. The ROPA will be created / reviewed by the DPO.	Corporate Legal Manager and service representatives – 2019/20
Medium	**Members' Information** Council information held by members has been largely identified. However, one councillor stated that they share information with third parties and do not have appropriate access controls when storing the information at their home. ***Risk**: Personal data may be compromised if appropriate security and control measures are not in place.*	This will be followed up with the Head of Democracy, Strategy and Partnerships, in consultation with the Project Team.	Head of Democracy, Strategy and Partnership and the Project team – November 2018
Medium	**Privacy Notices** Three out of two hundred and ten privacy notices have not been written by services and there are twelve awaiting review by the DPO. The highest risk area without a privacy notice is Members.	The Project Team is to review these with individual service reps, to clear the outstanding.	Corporate Legal Manager and Service representatives – March 2019

	***Risk**: The absence of a Privacy Notice means that the person providing the data is not clear on the purpose for which their information is obtained and how it will be processed.*		
Medium	**Historical Data** a) Rushmoor IT systems hold data going back many years, of which some may be unnecessary. Manual records across services could also hold outdated and excessive information. The 'Tidy Friday' initiative proved a popular and effective method of staff reviewing their records and disposing of them accordingly. b) The GDPR principle of 'data protection by design and default' should be considered in the review of historical information. Technical measures such as 'pseudonymisation', 'anonymisation' and 'minimisation' could be implemented or built in to systems. ***Risk**: Work on data requests can be unnecessarily prolonged and use additional resources due to the superfluous data held.*	Work is continuing within IT. There is on-going work to update Rushmoor applications with GDPR modules / functionality. Note – There is a large resource implication for this task and the application support team have to focus on current priorities. Priority will be given to the high-risk systems / sensitive data.	Head of IT & Facilities – 2019/20
Medium	**Data Protection Policy** a) The Data Protection Policy is held on the intranet but is out of date with the latest version indicating issue in 2002. b) The 'Data Protection' page within the Staff Handbook on the intranet is out of date. ***Risk**: In the event of a breach, it could not be proven that the council had taken all reasonable steps to ensure good awareness for all management, officers and Members.*	The Data Protection Policy will be reviewed and updated by Legal.	Corporate Legal Manager and Audit Manager – June 2019

Low	**Retention guidelines** There is no nominated officer to ensure that the retention schedules, maintained by managers, remain updated. This could fall within the remit of the new Data Protection Officer. ***Risk**: Guidelines may fail to be updated in accordance with statutory retention periods.*	This will be managed by the DPO.	Corporate Legal Manager – November 2018
Low	**Data Breach Log** There is no specific log of data breaches that have occurred, documenting the risk to individuals and a decision to notify the ICO. ***Risk**: The council may fail to maintain an auditable record of data breaches and consider potential risks to individuals.*	The Project Team is aware and this is being created.	Legal Services Manager – November 2018
Medium	**Data Protection Impact Assessments** A DPIA has been undertaken for one service, but are outstanding for others. A DPIA template exists, but it is not clear how this is currently being utilised. ***Risk**: Risks to individuals may fail to be considered when processing personal information.*	A project is being identified to pilot the template on. The Project Team will work with the service reps.	Project team/ Service representatives – January 2019
Medium	**Third Party presence in offices** The Citizens Advice Bureau (CAB) are to be based within the council offices. A DPIA has not been completed to mitigate any risk. ***Risk:** The CAB proximity to council staff and vice versa creates a risk of customers' personal*	The DPIA will be undertaken.	Head of IT & Facilities – January 2019

	information being viewed/obtained by third parties.		
Medium	**Contracts** To progress the updating of wording on existing contracts and supplier documentation, guidance is required to be provided to the officers. This includes the major Leisure Contract renewal. ***Risk**: Contract and supplier documentation may not be GDPR compliant.*	The Procurement team needs advice / guidance from the DPO to update contract documentation and templates.	Corporate Legal Manager and Principle Procurement Officer – January 2019
Medium	**Data Sharing Agreements** The Data Sharing Agreements (with third parties) across council have been identified, but need to be reviewed to ensure they are up to date to meet compliance with GDPR. ***Risk**: The extent of Data Sharing Agreements is not known and they may not be GDPR compliant.*	The Project Team will continue to gather information and work with the services.	Project team/ Corporate Legal Manager – 2019/20
Low	**Acceptable Use of IT Policy** This was last reviewed and updated in May 2017 in relation to PSN. This now needs to include the relevant GDPR aspects. ***Risk**: Staff may not be fully aware of their electronic data storage and sharing responsibilities under GDPR.*	New content to be developed between Legal, IT and Audit and to be published. This will be linked with the e-learning on GDPR.	Head of IT & Facilities – January 2019
Low	**Information Asset Owners** The role of Information Asset Owners is not formally documented, along with its reporting lines to the Data Protection Officer and Senior Information Risk Owner.	It is understood that work to progress this is underway and will be progressed at the next service rep meeting.	Corporate Legal Manager – January 2019

	***Risk**: The council's information governance framework is weakened if the Information Asset Owner role is not formally documented.*		
Medium	**Data Protection Officer** This statutory role is currently being covered by the Legal Services Manager as an 'interim' role since the Solicitor to the Council left. A Data Protection Officer has not formally been appointed but is due to be considered once the new Corporate Legal Manager starts in November 2018. ***Risk:** The council do not currently have an officially designated Data Protection Officer.*	The DPO role has been appointed and commences November 2019.	Corporate Legal Manager – November 2018

Audit Title 3	**Cyber security - follow up**		
Year of Audit	2018/19		
Assurance given at time of the audit	**Reasonable** - *Basic controls designed to achieve the system/function/process objectives, are in place. Improvements are required if key controls are to be established.*		
Assurance given at time of the follow up	**Reasonable** - *Basic controls designed to achieve the system/function/process objectives, are in place. Improvements are required if key controls are to be established.*		
Overview of area	An audit was carried out on Cyber-security in October 2017. The audit found that there are processes in place to address security vulnerabilities and an anti-ransomware tool is utilised to prevent the malicious encryption of data files. The findings from this audit resulted in 6 medium priority recommendations being made which were agreed by management.		
Priority	**Way forward agreed**	**Follow up findings**	**Recommendation status**
Medium	Whilst the Legal Services Manager performs some duties associated with the GDPR's definition of the Data Protection Officer role, there are some vital elements that are not currently performed. Therefore, it is important that the Legal Services Manager receives a clear outline of all expected DPO responsibilities. A decision must then be made about who will fulfil this statutory function post-May 2018 (i.e; current DPO/shared function with another officer or another local authority etc.).	The GDPR Governance board confirmed that the DPO role is part of the new Corporate Legal Services Manager role. Therefore, the vital elements of the Data Protection Officer will be carried out when she is in post in November 2018.	Implemented

Medium	The Council operates a General Data Protection Regulation (GDPR) Working Group. Using guidance provided by the Information Commissioner's Office (https://ico.org.uk/for-organisations/data-protection-reform) as a basic structure, an action plan should be drafted focusing on key areas of change and identifying action owners within the organisation. A draft GDPR Action Plan used by another local authority has been provided to the Data Protection Officer and IT Technical Services Manager for reference. It may also be an option to contact other local authorities in the area (or even Hampshire County Council) and organise a meeting to compare scheduled activities.	A GDPR specific audit has been carried out. The findings identified that an action plan is in place, which focuses on key areas of change and has identified action owners within the Council.	Implemented
Medium	The Council's Acceptable Use of IT Policy (AUP) requires a personal declaration by Members and Temporary Staff confirming they have received and read a copy of the policy, yet there is no process in place regarding New or Existing employees. It is recommended that the AUP is communicated to all employees who must confirm their understanding of, and adherence to, the policy. Human Resources should retain a permanent copy (physical or electronic) of this signed declaration attached to employees' records. Consideration should be given to how frequently employees should be refreshed, and it is advised that this is on an annual basis.	The AUP is being updated in conjunction with Internal Audit, as part of the GDPR project. The personal declaration form will be updated as part of this. Consideration will also be given to the frequency of providing employees with a refresher of the AUP requirements.	Not implemented but work is currently underway

Medium	With the General Data Protection Regulation (GDPR) replacing the current Data Protection Act as of May 2018, it is advised that Data Protection training for all staff is performed on a mandatory basis. There may be an opportunity to identify a suitable e-learning module that can be disseminated to all employees and tracked via a suitable mechanism similar to how Health & Safety education is tracked within the Council.	Data Protection training has been reviewed however, the module which was being trialled could not be fully integrated with the e-learning training system currently in place. The GDPR Governance board has agreed that the current e-learning system can be used for internal online training for staff. The Legal Services Manager will identify suitable GDPR content (either from other local authorities or by licence) and this can then be set up on the existing e-learning system. Therefore, formal training has not yet been given to staff, however one day training has been given to Managers and Members relating to GDPR. Formal Member training is arranged for late 2018/ early 2019.	Not implemented but work is currently underway by the Legal Services Manager.
Medium	The IT Technical Services Manager is currently validating an Information Security e-learning module with an intention to deploy this education to all users within the council. It is strongly recommended that this education is mandatory and has the same level of focus as other significant employee risks, such as Fire Awareness and Health & Safety learning.	An e-learning module has been rolled out to all employees in 2018. This is tracked to show who has completed the module and reminders are issued for completion. This will be carried out annually in a similar way to the Health & Safety education.	Implemented

Medium	Remote/Home Workers currently have the ability to turn off Location Settings and the Sophos Mobile Console cannot “force” these settings to be permanently active. This means that controls in place on the SMC designed to secure the device, should it be lost or stolen, are rendered ineffective. IT Services is advised to require Location Settings to be permanently enabled to be compliant with Mobile Device Management.	The location settings have now been enabled and if location settings are turned off then the device is no longer compliant.	Implemented