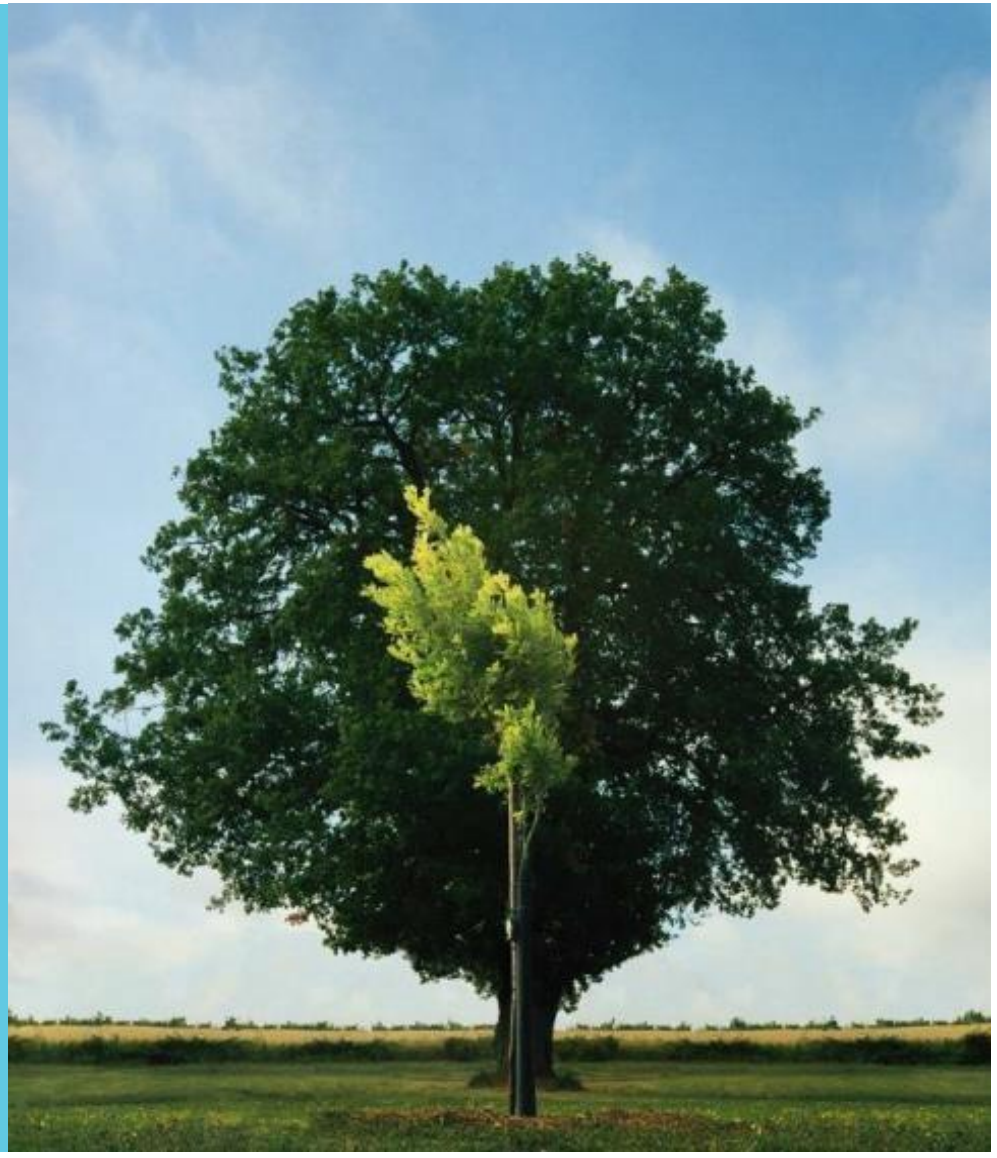
OXFORD CITY COUNCIL

INTERNAL AUDIT FOLLOW UP OF RECOMMENDATIONS REPORT

December 2017



INTRODUCTION AND EXECUTIVE SUMMARY

Introduction

Ahead of each Audit and Governance Committee we follow-up those recommendations raised by Internal Audit which are due for implementation. We request commentary by responsible officers on the progress to our recommendations and for those High and Medium recommendations due we verify progress to source evidence and conclude either that the recommendation is complete or incomplete.

There were **21** recommendations due for December 2017 comprising of Two High recommendations and 19 Medium recommendations.

Executive Summary

Please find below a summary of the **21** recommendations that were due for completion prior to the January 2018 Audit and Governance Committee:

2015 - 2016 Recommendations

- Two Medium recommendations have been implemented and can be removed from the Recommendations Tracker

2016 - 2017 Recommendations

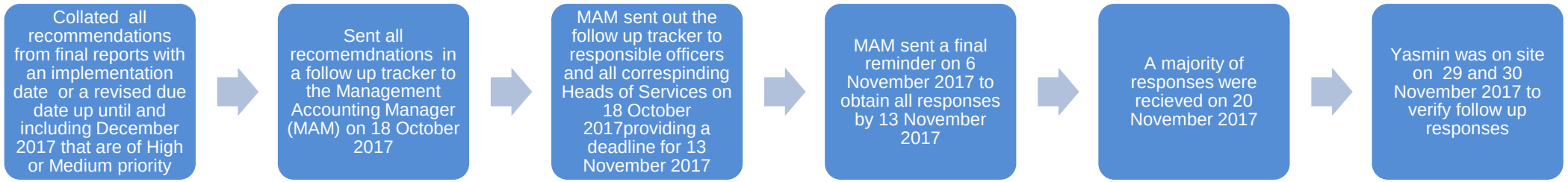
- Two High and Eight Medium recommendations have been implemented and can be removed from the Recommendations Tracker
- Five Medium recommendations are not complete and have all been given a first, second, third or fourth revised due date. These recommendations will continue to be followed up until they are complete we will:
  1. Continue to emphasise to staff to be realistic about the implementation dates when completing their management responses at the completion stage of each internal audit review
  2. Issue the recommendations tracker to all the relevant Heads of services on a monthly basis from the December audit committee onwards
  3. Issue reminder emails 6 weeks prior to the follow up review to ensure timely completion of each recommendation

- One Medium recommendation has been downgraded to a low level recommendation and therefore removed from the Follow up tracker

2017 - 2018 Recommendations

- Three Medium recommendations have been implemented and can be removed from the Recommendations Tracker

Flowchart of the follow up process – below we have included a process flow chart to explain how follow up responses are obtained timescales are achieved



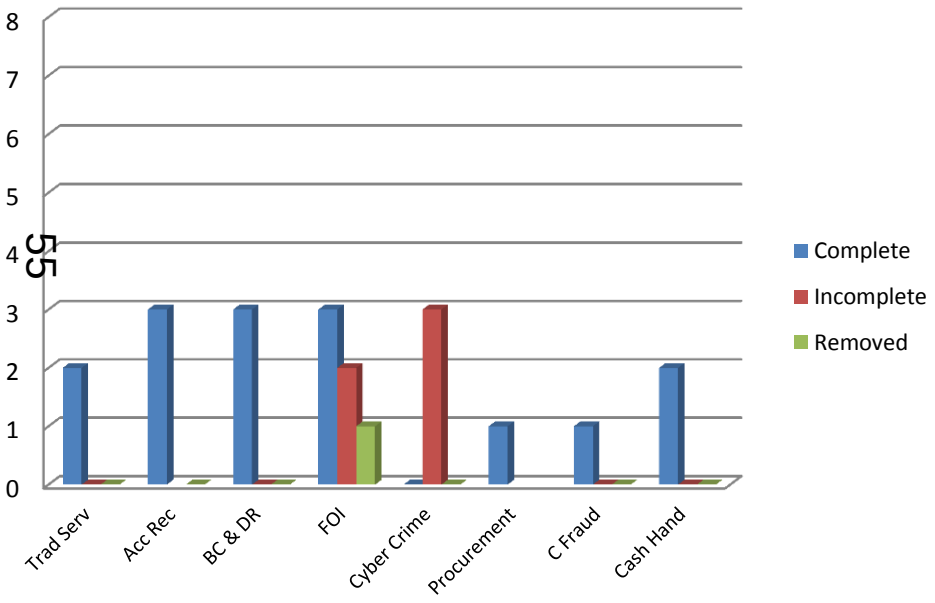
INTRODUCTION AND EXECUTIVE SUMMARY

The charts below reference the number of recommendations due up until and including December 2017. In total there were **21** recommendations due for follow up, chart 1 demonstrates the number of recommendations due for December 2017 of which, **15** recommendations were complete **5** were incomplete and **1** removed.

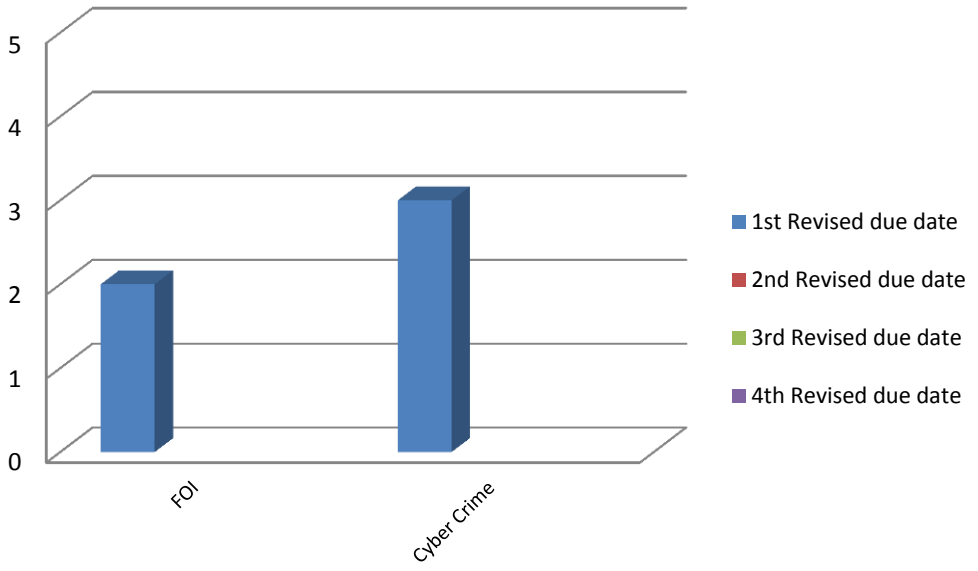
Chart 2 demonstrates the number of recommendations incomplete; of the **21** recommendations **5** were incomplete. We issued **5** recommendations with a first revised due date this was for Cyber Crime and Freedom of Information.

.

1. The status of 21 recommendations due for December 2017



2. Five Recommendations due for December 2017 with a revised due date issued for the 1st, 2nd, 3rd or 4th time



Please note the number of incomplete recommendations have decreased in comparison to the previous Follow up report issued in September 2017:

Month	No. of Recommendations incomplete	No. of Recommendations complete	% of recommendations incomplete (Incomplete/Total Recommendations)
June 2017	14	26	35% (14/40)
Sept 2017	10	25	29% (10/35)
Dec 2017	5	15	23% (5/21)

RECOMMENDATIONS COMPLETE

Audit	Recommendation made with reference to the corresponding Internal Audit report	Priority Level	Manager Responsible	Head of Service	Original Due Date	Notes on Completion
2015 – 16 Trading Services	2a) A proposal should be tabled in agreement with the Trading Board and Recruitment which details the challenges and options for resolving the challenges 2b) Formal succession planning actions should be drafted and approved by the Trading Board for critical areas of reliance on critical personnel.	M	Graham Bourton, Head of Direct Services	Graham Bourton, Head of Direct Services	~~Nov - 16~~ Nov - 17	We verified that the succession plan was defined and agreed with the trading board and recruitment. The succession plan detailed challenges trading service are exposed to and options available for resolving these challenges. Furthermore, a new head of service has been appointed to manage the succession action plan going forward.
2016 – 17 Business Continuity and Disaster Recovery	5) Management should require that the Council's business continuity and disaster recovery plans are tested on at least an annual basis or following a significant change. The results of all testing performed should be reported to senior management for review.	M	Bill Lewis, Financial Accounting Manager	Nigel Kennedy, s151 Officer	Dec - 17	A full review of the Councils service BCPs and corporate BCP has been undertaken with the assistance of Zurich, the Councils insurance and risk advisors. This started with a workshop with all Heads of Service on 23rd May, followed by a review of all plans which were then further reviewed by Zurich to ensure that these were robust. A date for the test of plans has been scheduled for 18th October 2017.
2016 – 17 Business Continuity and Disaster Recovery	6) Management should review the use of its Horspath Road offices to support the continuity of its critical services. Where necessary, management should consider identifying alternative locations or the use of remote working facilities. Business continuity plans should be updated to include how members of staff would get to and from its alternative locations in the event of an incident.	M	Bill Lewis, Financial Accounting Manager	Nigel Kennedy, s151 Officer	Dec - 17	

RECOMMENDATIONS COMPLETE

Audit	Recommendation made with reference to the corresponding Internal Audit report	Priority Level	Manager Responsible	Head of Service	Original Due Date	Notes on Completion
2016 – 17 Business Continuity and Disaster Recovery	4) Senior Management must produce a defined IT Disaster Recovery Plan that is aligned to the Council's continuity arrangements and includes, but is not limited to: •The recovery time and recovery point objectives for IT infrastructure and systems •The procedures for invoking the Plan in the event of a disaster •The procedures and information necessary for communicating with all key members of staff within IT and the wider Council •The procedures for recovering the Council's critical IT infrastructure and systems •The contact information for all third party IT suppliers. Furthermore, Senior Management should require that all third parties involved in the recovery of the Council's IT arrangements provide assurance that their disaster recovery plans are adequate.	H	Helen Bishop, Head of ICT	Nigel Kennedy, s151 Officer	~~Mar – 17~~ Sept - 17	We verified that two Disaster Recovery test scenarios have been completed with SCC at their recovery centre in Birmingham within the last 6 months. The initial test was limited in scope to test the recovery process and obtain confidence that the procedures were in place to affect a recovery. This was completed successfully in March 2017. In October 2017 the council completed a full test of the entire key Infrastructure and Applications environment, with the exception of a small number of specialist production servers that could not be tested in a non-service-impacting way. The output of this has been to inform the DR arrangements within the Operational Manual (Part of the contract), SCC are currently drafting this for OCC for inclusion within the DR and BCP plans. DR and BCP plans are now in place and include a schedule for loading ICT infrastructure and application servers, and have been previously shared with BDO, and are currently under review within not only the ICT department, but in the wider context of a council wide BCP review exercise.

RECOMMENDATIONS COMPLETE

Audit	Recommendation made with reference to the corresponding Internal Audit report	Priority Level	Manager Responsible	Head of Service	Original Due Date	Notes on Completion
2016 – 17 Freedom of Information	1a) The Council should introduce a streamlined approach to process FOI requests. Please see a recommended process flow chart in Appendix I 1b) Each service area should nominate an FOI champion to handle FOI requests who is not the Head of Service	M	Mike Newman, Corporate Affairs Lead	Lindsay Cane, Head of Law and Governance	Oct - 17	1a) We verified that a streamlined approach has been agreed by the Corporate Affairs lead and the Head of Law and Governance. This is in line with the process flow chart recommended by Internal Audit. 1b) Although there are two heads of services that remain as champions, there are now nominated champions for each service area. The list of champions is circulated within training sessions
2016 – 17 Freedom of Information	2a) The Council should designate at least one further individual to be trained and supported to manage the FOI process. Should the FICO be absent the following teams should be considered: Support from the Corporate Affairs Lead (current arrangement) The PA team Law and Governance Support Staff	M	Mike Newman, Corporate Affairs Lead	Lindsay Cane, Head of Law and Governance	~~Jul – 17~~ Nov - 17	The head of service has identified that the Law and Governance support staff will manage and support FOI requests, should the FICO be absent from duties. Duties have been approved by the Head of Law and Governance and arrangements are now in place for the Law and Governance support staff to access the FOI system.
2016 – 17 Procurement	1) The Council ensure that they have an adequate electronic procurement system in place.	H	Amanda Durnan, Strategic Procurement and payments Manager	Nigel Kennedy, s151 Officer	Nov - 17	We verified that there is now an electronic procurement system in place called Pro – Contract. There have been no issues with the new procurement system this far.

RECOMMENDATIONS COMPLETE

Audit	Recommendation made with reference to the corresponding Internal Audit report	Priority Level	Manager Responsible	Head of Service	Original Due Date	Notes on Completion
2016 – 17 Accounts Receivable	2a) The requirement to perform Customer Due Diligence (CCD) checks must be communicated to all relevant staff setting out the consequences to the Council of non-compliance with legislation 2c) As part of the Agresso milestone 6 upgrade (due in March 2017) the Council should enforce a parameter whereby, staff are prompted to ensure that CDD checks have been completed and/or considered prior to submission for authorisation.	M	Neil Markham, Incomes Team Leader	Nigel Kennedy, s151 Officer	~~Mar – 17~~ ~~Sept – 17~~ Oct - 17	The Customer Due Diligence was published in Council Matter on November 28th. Discussion within the Trade Waste / Incomes meeting were around communicating the criteria for photo id and proof of address as a requirement from all new customers. 2c) A due diligence box has now been created within the system. Allowing all income officers to check and essentially tick the due diligence box to verify that appropriate checks have been performed.
2016 – 17 Accounts Receivable	3b) Income officers should seek to review the customer creation forms or confirm that they were completed on the creation of a customer	M	Neil Markham, Incomes Team Leader	Nigel Kennedy, s151 Officer	~~Mar – 17~~ ~~Sept – 17~~ Nov - 17	A Customer Amendment Logging Report has been created where it produces a list of all incomes officers who approved the customer creation and the officer who created the customer account on the system. The report has been saved in the following location: M:\Financial-Management-Capital-Strategy\Agresso Report Library\MS4 - from Feb-16\Accounts Receivable and will be produced on a monthly basis for the Incomes team leader to review.

RECOMMENDATIONS COMPLETE

Audit	Recommendation made with reference to the corresponding Internal Audit report	Priority Level	Manager Responsible	Head of Service	Original Due Date	Notes on Completion
2017 - 18 Counter Fraud	2) Gap analyses of staff resource and current IT capability should be performed to identify any risks to achieving the annual Investigation Service work-plan, so that actions to mitigate these may be planned for in good time.	M	Scott Warner, Investigations Manager	Nigel Kennedy, s151 Officer	Dec - 17	A business case to propose an enhanced Investigation Team structure has been prepared and submitted to both CEB and One Council Board. The case received full approval at CEB and provisional approval at One Council Board. The case proposes conversion of fixed-term contract staff to permanent establishment posts as well as increased staffing levels on the team to address risk and resilience issues in dealing with team targets as well as commitment to external trading obligations. Additionally, a recruitment campaign for an additional staff member to the existing establishment has recently concluded with a successful appointment.
2017 – 18 Cash Handling	1) Cash tins should be held securely with the key kept separately from the cash box at all times. Include operating procedures for the security controls over the cash boxes. (See recommendation 2 for the procedure note recommendation)	M	Amanda Durnan, Strategic Procurement and payments Manager	Nigel Kennedy, s151 Officer	Sept - 17	We verified that cash tins are held securely and keys are kept separately from the cash box.
2017 – 18 Cash Handling	2) Procedure notes should be designed to instruct teams on cash handling functions, including the frequency of depositing cheques with finance. Provide cash handling leads with refresher training on the findings and recommendations identified as part of this review. Carry out local audits to ensure services are compliant with the agreed procedures	M	Amanda Durnan, Strategic Procurement and payments Manager	Nigel Kennedy, s151 Officer	Sept - 17	Procedure notes are issued and updated on the council intranet - local audits are outside of the Accounts payables remit therefore instructions have been passed to all Service Heads so they can audit their corresponding areas.

RECOMMENDATIONS INCOMPLETE

Audit	Recommendation made with reference to the corresponding Internal Audit report	Priority Level	Manager Responsible	Head of Service	Due Date	Progress to Date	Revised Due Date
2016 – 17 Freedom of Information	4a) Once the reporting is improved this can help inform the agreement of service area Publication Schemes 4b) The Council should adopt the following measures to aid further transparency: Create a platform similar to the 'What do they know' website for select FOI requests Prior to creating an FOI request, prompt the user on whether common subject matters regarding FOI requests have been considered A key word search identifier should be on the FOI request page, where certain key words within the request pop up links to relevant Council pages.	M	Milke Newman, Corporate Affairs Lead	Lindsay Cane, Head of Law and Governance	~~Dec - 17~~	4a) This is currently in progress and will be addressed in Jan – 18. 4b) Currently reviewing the best approach to create a platform for a publication scheme. The Council are still using the intranet as a current platform to aid transparency.	Jan - 18

RECOMMENDATIONS INCOMPLETE

Audit	Recommendation made with reference to the corresponding Internal Audit report	Priority Level	Manager Responsible	Head of Service	Due Date	Progress to Date	Revised Due Date
2016 – 17 Cyber Crime	2) Management should review and, where necessary, revise the Council's Information Security policy so that it is reflective of existing ways of working. The policy should include, but not be limited to: The responsibilities of all stakeholders with regards to information security, including information asset owners The roles, responsibilities and arrangements that exist between the Council and SCC The procedure for classifying information assets The Council's acceptable use standards The actions to be taken by all parties following the identification of an information security incident.	M	Vic Frewin, Chief Technology and Information Officer	Helen Bishop, Head of ICT	~~Oct - 17~~	Information Security Policy is currently being revised to incorporate additional guidance for users associated with GDPR and cyber security. The SCC Sentinel Platform as a Service solution provides full assurance regarding data security, and is regularly audited and certified. These assurances will be incorporated into the policy. Acceptable Use Policy is also currently under review by the GDPR project team. Changes will be incorporated into the InfoSec policy. The Security Incident currently being evaluated as part of BCP review.	Mar - 18

RECOMMENDATIONS INCOMPLETE

Audit	Recommendation made with reference to the corresponding Internal Audit report	Priority Level	Manager Responsible	Head of Service	Due Date	Progress to Date	Revised Due Date
2016 – 17 Cyber Crime	3) The Council's draft Information Asset Register should be updated to include: The security controls that have been applied to secure each information asset The at-rest location of each information asset The classification applied to each information asset, in line with the Council's and the Government's Security Classification standards. All required information should be recorded for each information asset. The Information Asset Register should be reviewed and approved by Senior Management and then communicated to all relevant stakeholders.	M	Vic Frewin, Chief Technology and Information Officer	Helen Bishop, Head of ICT	~~Oct - 17~~	Asset register is currently being reviewed and audited for completeness, and current asset data is undergoing full review. All data is secured at rest within PSN accredited platform (Sentinel) hosted by SCC All assets are being assessed to identify the correct security assessment of classification. This will be recorded in the asset register, reviewed and distributed.	Mar - 18
2016 – 17 Cyber Crime	4) The training that is provided to all members of staff should be reviewed and updated so that it makes specific reference to information and cyber security issues. This should include, but not be limited to: How to prevent an incident from occurring, such as not responding to emails from unknown or untrusted sources The actions to be taken when a breach is detected.	M	Vic Frewin, Chief Technology and Information Officer	Helen Bishop, Head of ICT	~~Oct - 17~~	Current training materials are currently being reviewed and updated with additional GDPR and Cyber Security guidance. GDPR training sessions are being rolled out. Staff notifications are sent in real-time as response to incidents as they unfold. This retains focus. Permanent guidance is available on intranet and via ICT help desk.	Mar - 18

RECOMMENDATIONS REMOVED

Audit	Recommendation made with reference to the corresponding Internal Audit report	Priority Level	Manager Responsible	Head of Service	Due Date	Reason for change of priority level from High to Low or Removal
2016 -17 FOI	1c) Heads of Service should agree on a risk based approach to inform their oversight of FOI requests: Apply a risk based approach to FOI requests i.e. an agreed narrative which helps inform the risk of an FOI request. This may cover risks such as who the requester of the FOI is, if it involves a Member or if it could result in high levels of public scrutiny Each case should be flagged as either High, Medium or Low. Those which are High, must receive approval from the Heads of Service. Those which are Medium and Low should be approved by the FOI Champion.	M → L	Milke Newman, Corporate Affairs Lead	Lindsay Cane, Head of Law and Governance	~~Oct - 17~~	The Council are currently trying to agree the best approach in adopting a risk based methodology. Management are wary of trying to refrain from rating each FOI case leading to a level of prioritisation as they are all deemed as priority level cases. All risks are rated as high if they exceed 20 working days timescales. Therefore, discussions are currently underway on the best approach to take. In addition, there are a very small number of cases that are not dealt within 20 working days therefore the risk of not responding to these cases in a timely manner is small. As a result, we have revised this recommendation to be a low level recommendation.

This page is intentionally left blank